SCHEDULE Q

CONTRACTOR'S SOLUTION

CONTENTS

SCHEDULE Q, PART A

CONTRACTOR'S SOLUTION

CONTENTS

1 INTRODUCTION

For the avoidance of doubt, should any conflict occur between Schedule Q, Part A (**Contractor's Solution**) and any other Contract Schedule then that other Contract Schedule shall take precedence.

2 MANAGEMENT METHODS

2.1 Project Management

2.1.1 Northrop Grumman shall be the Prime Contractor and systems integrator to meet the full range of IDENT1 requirements as specified in Schedule D (**Detailed Operational Requirements**).

2.1.2 The Contractor shall provide complete Contract and Subcontract management for:

(a) Automated Fingerprint Recognition (AFR), including multiple vendors.

(b) Maintenance, spares, logistics, and transportation.

(c) Wide Area Network (WAN) for England, Wales, and, where applicable, Scotland.

(d) Livescan for England, Wales, and, where applicable, Scotland.

2.1.3 The Contractor's team shall include, at Contract commencement, the following subcontractors who shall be known as Material Subcontractors:

SUBCONTRACTOR	PRIMARY ROLE ON IDENT1
SAGEM	AFIS Technology
Phoenix IT Services	Hardware Maintenance and Installation
Energis	WAN Communications Provider
Smiths Heimann Biometrics	Livescan Provider

2.1.4 Any changes to the above-listed Material Subcontractors are subject to the prior agreement of the Authority, as set out in Schedule B (**Conditions of Contract**), which consent shall not unreasonably be withheld.

2.1.5 In order to minimise programme transition and delivery risk, the Contractor's team shall include key management staff who have had direct experience with the current National Automated Fingerprint Identification System (NAFIS) Services design, development, and operations and relevant programme experience with the Authority and IDENT1 Services users.

2.1.6 The Contractor shall participate in monthly Programme Status Reviews (PSRs) (see Schedule O:12 (**Documentation**) and Schedule I (**Contract Management**)) with the Authority. PSRs shall be conducted at Authority locations in the UK, unless mutually agreed upon otherwise. The Contractor shall ensure that the above-listed Material Subcontractors shall also be available to attend such reviews when required by the Authority.

2.1.7 The Contractor shall develop an IDENT1 service plan (as part of Schedule O:58 (**Documentation**)) that meets the IDENT1 Services programme needs and is based

on an evolution of the current NAFIS Services. This plan shall address methods to avoid disruption to ongoing service delivery and minimise impact on users.

2.1.8 The Contractor shall manage the entire IDENT1 Service in accordance with Contractor policies that are comparable to PRINCE2 methodology, including exception management and reporting.

2.1.9 The Contractor shall conduct quarterly internally independent project reviews by the Contractor's Project Review Authority (PRA) of the technical, schedule, and cost performance of the programme. A summary of the outcome of any PRA shall be included for discussion, where appropriate, at the next PSR or more urgently as required.

2.1.10 The Contractor shall conduct monthly status reviews with its Material Subcontractors.

2.1.11 The Contractor shall employ a range of its internally approved management tools to assist programme managers in the management of the IDENT1 Services. At a minimum, the Contractor shall use a requirements management tool (DOORS or equivalent) approved by the Authority and a configuration database tool (Accurev or equivalent).

2.1.12 The Contractor shall manage the delivery of requirements and will provide the interface to the Authority through which these will be shared (See Schedule O:33 **(Documentation)**). The Authority will hold the master copy of the requirements baseline.

2.1.13 The Contractor shall implement a Risk Management Board (RMB), chaired by the Contractor's Systems Engineering Manager. This board shall be responsible for identification of risks; assessment of risk; and planning, selecting, and monitoring mitigation approaches. Outputs from the RMB shall be presented at the PSRs held monthly with the Authority, including full details of high-category risks.

2.2 Project Organisation

2.2.1 In order to mimimise programme transition and delivery risk, the Contractor's team shall include key management staff who have direct experience with the current NAFIS design, development, and operations and relevant programme experience with the Authority and IDENT1 users.

2.2.2 The following positions ("Key Contractor Positions") shall be staffed by Contractor staff ("Key Contractor Personnel") who shall not be substituted except in accordance with the provisions of Clause 6 of Schedule M (**HR and TUPE**).

Key Contractor Positions	Key Contractor Personnel
Programme Director	Rod Forry
Deputy Programme Manager	Richard Ginnett
Chief Engineer/System Architect	Phil Pedersen
Systems Engineering Manager	James Ling
Development Manager	Gerald Munizza
Service Delivery Manager	Mark Woodhouse
Quality Assurance Manager	Mark Keiffer
Transition Manager	Richard Ginnett (acting)
User Advocate	William Taylor
Contracts Manager	Karen Hatcher

2.2.3 The Contractor's Programme Director shall have overall responsibility for and authorisation to direct resources for the successful management and delivery of IDENT1 Services to the Authority.

2.2.4 The Contractor shall, in coordination with the Authority, define interfaces and points of contact between Contractor's staff and the Authority's staff.

2.2.5 The Contractor shall ensure that roles and responsibilities are established and maintained for all Key Contractor Positions. The roles and responsibilities shall include the escalation path and escalation procedures for all key positions.

2.2.6 In order to assist in the management and delivery of IDENT1 Service in accordance with the Contract requirements, the Contractor will implement the following measures:

(a) The Contractor shall have a dedicated Implementation Manager for the Transition activity in Scotland.

(b) The Contractor's project organisation shall include a project support functional area that provides contract management, subcontract management, and business and finance management.

(c) The Contractor shall have a configuration management activity for the control and management of all IDENT1 Services project-related hardware, software, and project deliverables.

(d) The Contractor's project organisation shall include a Chief Engineer/System Architect to review and oversee requirements and interface definition, performance and capacity modelling, security, logistics, reliability, maintainability, availability analyses, and human factors analysis.

(e) The Contractor's project organisation shall include a development functional area to provide system development, application development, integration and test, and systems support. The Contractor's development organisation shall include co-located SAGEM technical staff at least until FOC.

(f) The Contractor's project organisation shall include a Systems Engineering functional area to provide requirements and interface definition; performance and capacity modelling; security; logistics; reliability; maintainability; availability analyses; and human factors analysis. The Contractor's Systems Engineering functional area shall include a System Security Officer.

(g) The Contractor's project organisation shall include a business process engineering capability. The Contractor's business engineering shall provide initial use case development for potential new functionality within IDENT1 Services. The Contractor's business process engineering activities shall be coordinated with the Authority. The results of these analyses and developments shall be provided to the Authority for consideration of implementation under formal change procedures in accordance with Schedule L (**Change Control Procedure**).

(h) The Contractor's project organisation shall include a Service Management function to provide daily operations to IDENT1 Services, including service desk, user support, and installation and maintenance support. The Contractor's Service Management function shall include regionally based

user support staff to provide onsite assistance to the user community, including training, deployment planning, and technical assistance.

(i) The Contractor shall establish a senior technology review board to provide technical vision in the areas of criminal justice, homeland security, identification, biometrics, display concepts, and security. The Contractor shall provide results of the findings and recommendations to the Authority. The Authority shall also be invited to a Contractor-hosted annual identification technology forum.

(j) The Authority shall be established as a full member of relevant Contractor or subcontractor technology user groups, including but not limited to the SAGEM User Group.

(k) The Authority's membership in the technology user groups described above shall be at no charge to the Authority, except that the Authority shall bear the costs for all associated travel, accommodations, subsistence, and out-of-pocket expenses incurred by it or its representatives should they attend.

2.3 Planning and Reporting

2.3.1 The following planning and reporting shall be carried out by the Contractor, the methods and means utilised to achieve this shall be as specified in Schedule D (**Detailed Operational Requirements**).

2.3.2 The IMS shall divide the IDENT1 Service deliverables into projects that shall be further subdivided into stages for development and implementation. Stage planning and reporting shall address exception planning, as appropriate.

2.3.3 The Contractor shall review each project with the Authority to obtain Authority approval of the approach, method of delivery, and acceptance criteria as detailed in the Contract.

2.3.4 In each project/stage plan, the Contractor shall include activity for regression testing and validation of requirements under controlled conditions.

2.3.5 The Contractor shall provide information on individual projects as well as overall programme status. Project status shall include identification of issues and risks. This information shall be provided in a PRINCE2-compliant format.

2.3.6 The Contractor shall develop a Risk Management Plan in accordance with Schedule O:14 (**Documentation**).

2.3.7 The Contractor shall develop a Risk Mitigation Plan for risks defined in the Risk Management Plan.

2.3.8 The Contractor shall conduct formal customer milestone reviews for each project.

2.3.9 The Contractor shall provide a list of product descriptions agreed upon as deliverables in the next Stage Plan in accordance with Schedule O:18 (**Documentation**).

2.3.10 The Contractor shall provide a Product Checklist as defined in the PRINCE2 methodology.

2.3.11 The Contractor shall work with the Authority to identify planning and reporting methods to reduce costs or improve schedules to the mutual benefit of both parties. Changes shall be agreed upon through the Programme Configuration Control Board (PCCB) as described in Schedule L (**Change Control Procedure**).

2.4 Communication

2.4.1 The Contractor shall present as part of the Programme Initiation Review a communication strategy which covers the following:

(a) Geographic dispersion of users.

(b) The variety of user roles and responsibilities.

(c) The differing business processes.

(d) Variations in training requirements.

(e) Implementation schedules that extend over calendar and fiscal years.

(f) Stakeholders from integrated external interfaces.

2.4.2 The Contractor shall provide the Authority with a Communication Plan in accordance with Schedule O:15 (**Documentation**).

2.4.3 The Contractor shall support and coordinate the execution of the Communication Plan with the Authority on a quarterly basis.

2.4.4 The Contractor's Communication Plan shall include the following items. The means of delivery and content of the items shall, except where otherwise required by the Contract, be determined by the Contractor working closely with the Authority and, where appropriate, with Authority approval:

(a) User Advocate. The Contractor shall provide a User Advocate to provide senior policing experience relating to the identification and criminal justice community. The User Advocate shall actively solicit user feedback on the needs and performance of the IDENT1 Service. The User Advocate shall not conduct direct marketing or sales activities, without prior approval and coordination with the Authority.

(b) Conferences. The Contractor shall attend national and international conferences relating to IDENT1. The Contractor shall be a sponsor of the National Fingerprint Conference.

(c) Newsletters. The Contractor shall produce and disseminate a semi-annual user newsletter, similar to the legacy *Ridgeway News*.

(d) Status Reports. The Contractor shall produce and disseminate status reports, usually weekly, but as frequently as necessary to keep users informed of system status and operational activities.

(e) Web Portal. The Contractor shall develop and maintain an IDENT1 web portal to provide authorised access to documentation, training materials and management data.

(f) Management Reviews. The Contractor shall hold regularly scheduled internal management reviews in accordance with company policies and monthly PSRs with the Authority.

(g) User Groups. The Contractor shall provide suitable staff to attend the following user groups, including but not limited to:

(i) IDENT1 User Group

(ii) Livescan Electronic Identification Unit (EIU) User Group

(iii) Training User Group

(iv) ACPO Regional User Meetings

(h) User Information Days. The Contractor shall conduct briefings for users at the Contractor's UK facilities for transition and rollout plans for new functionality.

2.4.5 The Contractor shall provide web portal access to the Authority to relevant IDENT1 Management Information System (MIS) data. The data shall be displayed using Business Objects, or equivalent COTS business intelligence tools. The Contractor shall deliver, install, and support a workstation at the Authority's premises for access to the MIS data.

2.4.6 The Contractor shall provide training to Authority users on the business intelligence tool(s) and will provide onsite assistance for the first month after installation.

2.5 Controls

2.5.1 The Contractor shall prepare a Programme Initiation Review Documentation as described in Schedule O:9 (**Documentation**).

2.5.2 The Contractor shall employ its own company standard tools and processes for monitoring, tracking, and controlling the implementation of IDENT1 Services.

2.5.3 The Contractor shall develop, deliver, and maintain an Integrated Master Schedule (IMS) that identifies all major projects and their associated stages. The Contractor shall report progress and tolerance conditions against the IMS. The Contractor shall use the Earned Value System as an integral aspect of its project control process and provide exception visibility to the Authority as agreed (see Schedule O:11 (**Documentation**)).

2.5.4 The Contractor shall provide an exception plan to the Authority within a week of an exception being identified.

2.5.5 The Contractor shall not proceed to the next stage (see Schedule O:18 (**Documentation**)) without approval from the Authority. Where approval is not granted, the Authority shall provide written notice of such rejection together with detailed reasons therefore within ten days (or as otherwise specified in Schedule H (**Acceptance Procedures**)).

2.5.6 The Contractor shall monitor and track task status on a weekly basis.

2.5.7 The Contractor shall support, as reasonably required, IDENT1 Project Boards. Senior contractor representation shall be provided at the Project Board, as required by the Authority as set out in Schedule I (**Contract Management**).

2.6 Quality

2.6.1 The Contractor's project QA organisation shall have an independent reporting channel to the Contractor's business unit.

2.6.2 The Quality Management System (QMS) used in the delivery of the IDENT1 Service shall be based on company standards that are compliant with ISO: 9001 and Capability Maturity Model Integration (CMMI) and updated as described in Schedule O:10 (**Documentation**).

2.6.3 The QMS shall define standards, methods, and processes that apply to the IDENT1 Service and provide procedures for maintaining compliance for the duration of the Contract.

2.6.4 The QMS shall comprise the following components: quality planning, quality training, Quality Control (QC), Corrective and Preventive Action System (CPAS), quality reviews, and quality system performance and improvement.

2.6.5 A Quality Plan for the programme shall be developed in accordance with Schedule O:10 (**Documentation**).

2.6.6 The Quality Plan shall be required to be approved by the Authority and maintained for the term of the contract.

2.6.7 The development plans for stages/projects shall describe quality requirements and activities specific to stages/projects.

2.6.8 The Contractor shall implement QC through scheduled evaluations and audits of process, product, and service delivery as specified in the Quality Plan as follows:

(a) The results of evaluations and audits shall be documented and all results shall be available for Authority review.

(b) Nonconformities shall be subject to corrective action.

2.6.9 A CPAS shall be established and used to manage actions logged in response to QC findings.

2.6.10 The Contractor shall conduct formal quality reviews whenever a significant change occurs throughout the term of the contract to include the service delivery phase.

2.6.11 The Contractor shall monitor and measure QMS performance against quality metrics as defined in the Quality Plan.

2.6.12 The Contractor shall report on QMS performance status as requested.

2.6.13 Based on the results of QMS performance assessments, the Contractor shall where reasonable to do so identify opportunities for QMS improvement.

2.6.14 The Contractor shall use structured methodologies of its choice for process improvement activities that management approves for implementation.

2.7 Change Management

2.7.1 The Contractor shall employ a formal change management process that is integrated with the Contractor's Configuration Management System. The Contractor shall propose and agree with the Authority on a configuration management process for the IDENT1 Service and document this in accordance with Schedule O:34 (**Documentation**) and subject to Schedule L (**Change Control Procedures**).

2.7.2 Formal Contract changes shall be managed in accordance with procedures outlined in Schedule L (**Change Control Procedures**), which shall, where there is a conflict, take precedence over this part of this Schedule.

2.7.3 The Contractor shall apply change management to all configuration controlled items and baselines. The change control process shall be applied to IDENT1 hardware, software, and documents.

2.7.4 The Contractor shall maintain a Programme Configuration Control Board (PCCB) to control all system change requests. A list of proposed changes will be readily available to the Authority with detail of any Schedule and/or Quality impacts.

2.7.5 The Contractor's PCCB shall perform an assessment of each change request to evaluate:

(a) Operational impact of the change.

(b) Importance of the change.

(c) Cost, quality, and timescale impact of the change.

2.7.6 The Contractor shall ensure that approved changes are reflected in corresponding technical and programmatic documentation.

2.7.7 The Contractor shall apply audit controls to verify that following approved changes, the functional requirements are met and the physical content of changes are consistent with documentation.

2.7.8 The Contractor shall maintain configuration status controls to ensure that configuration items are maintained during all project phases and that changes are traceable to applicable products.

2.7.9 The Contractor shall ensure that where any changes adversely affect overall programme milestones, the IMS shall be updated by the next programme cycle.

2.7.10 The Contractor shall employ COTS tools in the change management process. The tools shall generate reports comparable to PRINCE2 reports to provide visibility of current information and to demonstrate completeness of product traceability to the required standard.

2.8 Delivery Management

2.8.1 The Contractor shall act as the design authority and service provider for the IDENT1 Services, working in the context of the Authority's overall IT strategies.

2.8.2 The Contractor shall develop/agree with the Authority a stage plan for each stage of the IDENT1 Services in accordance with Schedule O:18 (**Documentation**).

2.8.3 The Contractor shall provide project documentation to other groups as agreed with the Authority for information or review purposes.

3 SERVICE DELIVERY

3.1 Service Availability and Business Continuity

3.1.1 Availability

(a) The Contractor shall implement and deliver an Availability Management process that ensures that the IDENT1 Services meet the IDENT1 operational availability requirements. The Availability Management Process shall be ITIL compliant. The Contractor shall be responsible for full system availability, including the WAN as set out in Schedule F (**Service Level Requirements**). The Contractor shall be responsible for implementing system and component changes and enhancements, as may be required to meet system operational availability goals.

(b) The Contractor's Availability Management process shall incorporate key elements of the Contractor's existing design and support structure, including:

(i) Uninterruptible Power Supplies (UPSs) for IDENT1 kit at the Central Sites and Bureaux locations except where the UPS was provided by the bureau.

(ii) Distributed spares warehouses and supplies to reduce maintenance downtimes.

(iii) Onsite technicians at Contractor determined locations, based on availability and response time requirements.

(iv) Multiple test beds to evaluate new products and component reliability.

(c) The Contractor's availability management activities shall:

(i) Review and analyse availability requirements through its systems engineering process. This shall include the use of availability mathematical models, where appropriate.

(ii) Review impacts to business functions arising from availability issues, including identifying critical system components.

(iii) Set and review targets for availability, reliability, and maintainability of the IDENT1 Services system, including recovery time.

(iv) Monitor and evaluate availability trends.

(v) Investigate underlying reasons associated with availability issues.

(vi) Maintain and update an Availability Plan in accordance with Schedule O:63 (**Documentation**) that includes plans for availability improvements. This plan shall include periodic vendor assessments of current and new products and technologies.

(d) The Contractor shall designate an Availability Manager who shall interface with the Authority's Availability Manager for IDENT1. The Contractor's Availability Manager shall report to the Contractor's Service Delivery Manager.

(e) The Contractor's Availability Management process shall be an integral aspect of its overall Systems Engineering process to ensure that availability is considered within the IDENT1 life cycle.

(f) The Contractor's availability Management process shall include both operational data and engineering design assessments.

(g) The Contractor's Availability Management process shall include mechanisms for delivering increased system operational availability, primarily through the reduction of planned downtime.

(h) The Contractor's Availability Management process shall include mechanisms for communicating lack of availability and likely recovery period to appropriate users.

3.1.2 Business Continuity

(a) The Contractor shall provide Business Continuity Management as an integral aspect of its Systems Engineering process, a key element of which shall be IT Service Continuity Management. The Contractor shall implement Business Continuity Management in accordance with ITIL procedures.

(b) The Contractor shall develop, implement, and maintain a Business Continuity Plan as described in Schedule O:65 (**Documentation**).

(c) The Contractor's Business Continuity management shall be based on the existing NAFIS Services business continuity plans and procedures, including the Contractor's secondary site to provide intermediate and immediate recovery capabilities.

(d) IT Service continuity considerations shall be inherent in the design of the IDENT1 Services System.

(e) The Contractor shall ensure that Business Continuity management includes communication and coordination with the bureaux and addresses their local business continuity needs and plans.

(f) The Contractor shall coordinate IDENT1 Services business continuity planning with integrated external system interface providers.

(g) The Contractor shall conduct annual testing of the business continuity procedures, including integrated external system interfaces (see Schedule O:66 (**Documentation**)).

3.2 Service Management

3.2.1 The Contractor shall have in place ITIL-compliant service delivery systems and procedures for the term of the contract. These shall include but not be limited to:

(a) Service Level Management

(b) Availability Management

(c) Capacity Management

(d) Financial Management for IT Services

(e) IT service continuity management

3.2.2 The Contractor shall have in place ITIL-compliant service support systems and procedures for the term of the contract. These shall include but not be limited to:

(a) Configuration Management

(b) Change Management

(c) Incident Management

(d) Problem Management

(e) Release Management

3.2.3 The Contractor shall achieve BS 15000 or equivalent certification by its service delivery organisation by FOC, and shall maintain such certification for the duration of the Contract (see Schedule O:61 (**Documentation**)).

3.2.4 The Contractor shall ensure that new capabilities are integrated into the service management structure.

3.2.5 The Contractor shall manage all aspects of the delivery of IDENT1, providing availability to the users in accordance with Schedule F (**Service Level Requirements**) ensuring minimal disruption to the users. The Contractor shall ensure that staff involved in service delivery and service support have clearly defined roles and responsibilities, supported by role/job descriptions in accordance with contract requirements.

3.2.6 The Contractor shall carry out regular reviews of performance and service improvement initiatives.

3.3 Service Delivery

3.3.1 Service Level Management

Service provision shall be managed according to Schedule F (**Service Level Requirements**) (which in the event of conflict or inconsistency shall take precedence over this Schedule) and will cover the services and service levels to be delivered. The Service Level Requirement criteria shall cover:

(a) Search Accuracy

(b) Response Times

(c) Throughput

(d) Availability

(e) Support

(f) Other Service Quality Measures (to be agreed upon)

3.3.2 Measurement of overall performance shall include a measure of the effectiveness of the IDENT1 Service (e.g., the number of identifications and the timeliness with which they are made) in accordance with Schedule F (**Service Level Requirements**).

3.3.3 The Contractor shall provide the Authority with a monthly service report.

3.3.4 The SLR report shall be sufficiently detailed to demonstrate that the SLR requirements are being met and/or to report any exceptions.

3.3.5 The Contractor shall work with the Service Control Board to consider:

(a) Changes in working practices.

(b) The continued validity of measures.

(c) Improvement initiatives.

3.3.6 The Contractor shall develop and manage its own SLR's with its Subcontractors.

3.3.7 The Contractor shall develop SLR's with any third party provider of interfaces and shall seek Authority approval for associated SLR's (see Schedule O:62 (**Documentation**)).

3.4 Financial Management for IT Services

3.4.1 The Contractor shall have full financial responsibility for delivery of IDENT1 Service.

3.5 Service Support

The Contractor shall document their service support processes in the Operations and Maintenance Support Plan (see Schedule O:58 (**Documentation**)).

3.5.1 Incident Management

(a) All incidents reported to the service desk shall be logged on the service management support tool and an incident report created.

(b) All incidents shall be categorised and prioritised in accordance with Schedule F (**Service Level Requirements**).

(c) Calls shall be assessed and assigned to the appropriate member of the support team.

(d) Wherever incidents cannot be resolved by staff on the service desk, they will be escalated to second- or third-level support or assigned to a third-party subcontractor.

(e) Procedures shall support the escalation of incidents, either technically or hierarchically.

(f) A Work Log shall be maintained for each incident. All entries shall be time stamped and the identity of the individual making the entry shall be logged.

(g) The Work Log shall contain details of, for example:

(i) Investigative work undertaken.

(ii) Remedial action carried out.

(iii) Time taken to resolve the incident.

(iv) Interactions with the user.

(v) Association with a known problem if appropriate.

(h) The service desk shall provide users with updates on the status of incidents.

(i) Incidents shall only be closed after satisfactory resolution of the incident has been confirmed with the user who reported the incident.

(j) The service desk team leader shall monitor progress on incidents and maintain ownership of the incident through closure, to ensure that SLR response times are met.

(k) Procedures for incident resolution and any workarounds in place shall be contained in the Operations and Manintenance Support Plan (see Schedule O.58 (**Documentation**)).

(l) The Contractor shall define the process for reporting and managing major incidents. This process shall be documented in the Operations and Maintenance Support Plan (see Schedule O.58 (**Documentation**)).

3.5.2 Problem Management

(a) Problem management procedures shall be in place to detect underlying causes of an incident or incidents and to identify a path for resolution or prevention.

(b) Problem management shall be both proactive and reactive.

(c) Problems shall be logged in an Issues log, which shall contain details of, for example:

(i) Incident counts against the problem.

(ii) Workarounds in place.

(iii) Status of work on problem resolution.

(d) Following implementation of remedial action, the success of the implementation shall be measured and reviewed at the monthly contract review.

(e) The Contractor shall maintain an operations issue log, which contains a record of known system conditions which impact operations.

3.5.3 Release Management

(a) All new components introduced into the IDENT1 environment shall be subject to Release Management controls.

(b) All releases shall be planned to minimise the impact on the user community.

(c) Details of the contents of each release shall be maintained on the Configuration Management database.

(d) Each release shall be uniquely identified.

(e) Each release shall be built according to the documented build process.

(f) Each release shall undergo testing prior to acceptance (as set out in Schedule H (**Acceptance Procedures**)). This testing shall include:

(i) Functional Testing

(ii) Backward Compatibility

(iii) Regression Testing

(iv) SCR Thread Testing

(v) Interfaces

(vi) System Administration

(g) Backout plans shall be in place for each release.

(h) An ORR shall be held for each release to ensure that the following are in place:

(i) Deployment Schedule

(ii) Estimated Duration of Deployment

(iii) Estimate of Downtime

(iv) Resources

(v) Documentation

(vi) Operational Procedures

(vii) Details of Testing Carried Out

(viii) User Training

(ix) Operational Checkout Complete

(x) Release Notes

(xi) Backout Plans

(i) Progress and status of release deployment shall be tracked via a work ticket on the service management support tool.

3.5.4 Service Desk

(a) The Contractor shall provide a 24x7 service desk, which shall provide first-line incident support, day-to-day contact with users, help with using the service, and management information.

(b) Automated maintenance and support systems shall be in place for the service desk.

(c) The IDENT1 service desk shall be contactable by phone, fax, the IDENT1 user interface, and the service management support tool. Remote access to the IDENT1 Services system shall conform to CESG guidelines.

(d) The service desk shall provide regular updates to users on the status of current incidents. The Contractor shall have in place escalation procedures, allowing for calls to be passed to third-level and/or subcontractor support in a timely fashion, to ensure that incidents are handled effectively.

(e) The majority of support shall be provided from within the UK; however, the Contractor shall obtain Authority approval for any support required from outside the UK. The Contractor shall provide an alternate location for the service desk in the event of any downtime that may result in its being unavailable for more than four hours.

3.5.5 MIS Reporting

(a) The Contractor shall provide comprehensive MIS capabilities to the Authority to include measurement of the performance of the system against the SLR as set out in Schedule F (**Service Level Requirements**).

(b) The Contractor shall store audit data for at least two years online and up to 10 years of data in archive.

(c) The Contractor shall run acceptance tests with the Authority to ensure the validity of this data as set out in Schedule H (**Acceptance Procedures**).

(d) The Contractor will provide the Authority with access to all MIS data on the service being delivered.

(e) The Contractor will provide the Authority with its own workstation for the purposes of accessing MIS data.

(f) Users with appropriate access privileges shall be able to access MIS data.

(g) The level of data that users can access will be controlled by their access privileges.

(h) The Contractor will pilot an initial set of reports with the Authority and develop more comprehensive sets based on operational experience in accordance with the Contract.

3.5.6 Operations and Maintenance (O&M)

(a) The Contractor shall be responsible for the maintenance and support, including technology refreshes, of IDENT1 equipment, software, licences, infrastructure, and interfaces provided under this Contract to ensure compliance with the Service Levels set out in Schedule F (**Service Level**

Requirements). The following shall be carried out on a reasonable and as required basis in order to achieve this objective:

(i) The Contractor shall, wherever possible, avoid conflict between maintenance/release activities and Police Force events/initiatives.

(ii) The Contractor shall comply with Health and Safety and other appropriate legislation.

(iii) The Contractor shall review technological advancements and changes in standards and dependencies and make appropriate recommendations for change.

(iv) The Contractor shall provide a user support team, distributed across the country, to provide additional onsite support to the user community for the purposes of training; installation management, onsite support to the operations team, and general user liaison.

(v) The Contractor shall provide field support for installation and maintenance. This shall consist of centrally and regionally based staff.

(vi) Onsite maintenance resources shall be provided at Contractor selected operational sites.

(vii) The Contractor shall at its discretion and on a reasonable basis have in place remote spares holdings.

(viii) The Contractor shall ensure that day-to-day consumables, not provided under the Service are, wherever possible, readily available from a variety of commercial outlets.

(ix) The Contractor shall provide consumables of limited availability or high value.

4 OPERATIONAL ENVIRONMENT

4.1 Fingerprint Bureaux

4.1.1 The Contractor shall provide all IDENT1 equipment and accommodation modifications for the Bureaux of England, Wales and Scotland. The equipment shall include servers, workstations, monitors, peripherals, printers, scanners, local area networks, wide area network connections, desks, chairs, desk lighting, and UPSs for supplied equipment. The Contractor shall minimise the impact to the accommodations at Bureaux of England, Wales and Scotland.

4.1.2 The Contractor shall transition the existing Bureaux systems within the existing accommodations for space, weight, and power. The transition for the SAFR system shall be accomplished to the extent reasonably possible with the minimum interruption of operations during the transition. The Contractor shall provide temporary facilities for the transition of SAFR should it be necessary.

4.1.3 The Contractor shall agree with the Authority upon the specific configuration for workstation peripherals, for example, optical or magnetic tape and disk drives, prior

to installation at a Bureau. The rollout schedule for the workstations (quantity and timing) at the Bureau shall be agreed upon with the Authority and the Bureau.

4.1.4 The Contractor shall conduct site surveys for each IDENT1 Bureau in England, Wales and Scotland and define the specific accommodations needed at each Bureau. The Contractor shall document the results of the site survey in a Memorandum of Understanding (MOU) that documents the roles, responsibilities, and time lines for any planned site activity. The MOU shall be agreed upon with the Authority and the bureau (as set out in Schedule O:19 (**Documentation**)).

4.2 Custody Suites

4.2.1 The Contractor shall use reasonable efforts to support the Authority's efforts to obtain device approval for IDENT1 Livescan/EIUs in Scotland.

4.2.2 Accommodation planning shall be supported by a site survey, MOU, and project planning meetings. These activities shall ensure that any works to be carried out, and responsibility for those works, are clearly defined.

4.2.3 Plans for accommodation and site preparation shall be approved by individual forces and by the Authority.

4.2.4 The Contractor shall provide the Authority with documentation associated with accommodation planning.

4.2.5 Relocation of existing equipment in custody stations shall not be required.

4.2.6 The Contractor shall ensure that all equipment installed in Custody Suites:

(a) Shall not interfere with other equipment in the environment.

(b) Shall not pose a health and safety risk to staff in the suite.

(c) Shall not require a specialist environment.

4.3 Other Accommodation and Equipment

4.3.1 The Contractor shall obtain the Authority's approval of the location of all accommodation for the IDENT1 Services. All accommodation provided by the Contractor for the provision of the IDENT1 Services shall be physically secure in accordance with the security requirements in this Schedule Q and Schedule K (**Security**).

4.3.2 The Contractor shall provide the Authority with access to its IDENT1 facilities, by arrangement.

4.3.3 The Contractor shall ensure that the electrical supplies for centrally supplied service shall be supported by UPS and generator power supplies.

4.3.4 The Contractor shall ensure that equipment installed on its premises shall require no special environmental controls or building modifications, other than those normally expected for a data room.

4.3.5 Bureau equipment and any equipment on the Authority's premises provided by the Contractor for the provision of the IDENT1 Service shall be designed for operating in a normal office environment.

4.3.6 The Contractor shall provide Primary site and Secondary site facilities for the IDENT1 Service. The facilities at the Primary and Secondary sites shall be collectively referred to as the Central Facilities.

4.3.7 The Contractor shall provide a workstation at New Kings Beam House and at the Hendon Data Centre (HDC) for use by the Authority's personnel or designated other parties.

4.3.8 The Contractor shall provide a Bureau system (including a Livescan/EIU) at the Primary site. This Bureau system shall be used for the purposes of testing, demonstration and have the potential for use as a training system if required.

4.3.9 The Contractor shall provide a suite of equipment at the Secondary site facility for use as a demonstration and training facility. It shall also be used for the presentation of new functionality during user Information days.

4.3.10 The Contractor shall maintain a test and development environment in its Fairfax Facility in the USA.

5 LOCATION OF OPERATIONAL DATA

5.1.1 The Contractor shall provide data management functionality that focuses on availability, reliability, and consistency.

5.1.2 The Contractor shall maintain redundant copies of the Unified Collection and related data to ensure reliability.

5.1.3 The Contractor shall perform the following activities as an integral aspect of its operational activities in the UK:

(a) Archiving

(b) Backups

(c) Integrity checks

(d) Cleansing

5.1.4 Unless otherwise agreed with the Authority, the Contractor shall use non-operational data for all IDENT1 testing performed within its test and acceptance facilities..

5.1.5 If, under exceptional circumstances, a need arises to use operational data outside the operational system, the Contractor shall implement controls to protect the data from deliberate or accidental compromise.

5.1.6 The Contractor's System Security Officer (SSO) shall coordinate with, and seek the approval of, the Authority before any operational data are transmitted outside the system.

5.1.7 All operational data and information assets provided to the Contractor by or on behalf of the Authority shall, unless otherwise specified, remain the property of the Authority or, where applicable, of the party providing that information on behalf of the Authority.

5.1.8 The Contractor's SSO shall ensure that the rightful owner can recover all original or derived operational data and information assets.

5.1.9 The Contractor's SSO shall develop and ensure compliance with ISO 17799 policies for backup and recovery of all operational data and information assets, including in the event of unforeseen disasters.

5.1.10 The Contractor's SSO shall develop procedures in accordance with established policies for backup and recovery of operational data and information assets.

5.1.11 The Contractor shall train personnel on the security policies in place for the contract as follows:

(a) New staff shall be required to review programme security policies and procedures—including security and the Security Operating Procedures (SyOPs)—and to sign a certification acknowledging receipt and understanding of the documentation.

(b) Project personnel shall undergo annual security awareness training to ensure continuing compliance with the relevant security policies.

6 TRAINING

6.1 Training Systems

6.1.1 The Contractor shall provide and maintain training systems for the NTC for Scientific Support to Crime Investigation in Durham, the Metropolitan Police Fingerprint Training School in Hendon, and the proposed NTC training site in Wyboston, Bedfordshire.

6.1.2 The training systems shall mirror the full functionality of IDENT1 Services and shall be updated with all baseline IDENT1 functionality as it is deployed and shall provide a safe environment for students to be trained and practice Bureau operations.

6.1.3 The training systems configuration shall include one EIU, as installed in Custody Suites, at each of the three locations.

6.1.4 Each training system shall have its own discrete Print Set and Marks databases, together with other databases as appropriate for the functionality provided under IDENT1.

6.1.5 The configuration of the training systems, including databases, shall be deployed in accordance with the procedures detailed in the Contractor's Configuration Management Plan (as set out in Schedule O:34 (**Documentation**)).

6.1.6 Use of the training systems shall not impact the performance of other Bureau operations.

6.1.7 The Contractor shall provide training for the trainers at the training schools in the functionality of IDENT1. This shall include accreditation and ongoing assessment on an annual basis (as set out in Schedule O:27 (**Documentation**)).

6.1.8 The Contractor's design for the training systems, as a business continuity measure, shall provide for them to be reconfigured as an operational Bureau measure. This capability shall be implemented by FOC.

6.2 Ongoing Training of Users

6.2.1 The Contractor shall carry out a comprehensive Training Needs Analysis (TNA), as agreed upon with the Authority, at the commencement of the IDENT1 Services programme, which will feed directly into the Training Programme (as set out in Schedule O:29 (**Documentation**)).

6.2.2 Following completion of the TNA, the Contractor shall produce a Training Plan to be agreed upon with the Authority.

6.2.3 The Training Plan shall be produced as detailed in Schedule O:23 (**Documentation**). The TNA shall be reviewed by the Contractor and the Authority on an annual basis throughout the term of the Contract in order to ensure that the appropriate training has been identified and is being delivered to users and, further, that the training continues to be relevant and appropriate.

6.2.4 The Contractor shall design and develop training courses, in consultation with the Authority, for all baseline IDENT1 capabilities.

6.2.5 The Contractor shall maintain training records for the training courses that they carry out. These training records will include the courses and the specific personnel attending them which shall be available to the Authority if requested.

6.3 Transition Training

6.3.1 The Contractor shall provide training to FPOs in England and Wales on all new capabilities implemented within IDENT1, where this does not conflict with the strategy of the National Training school.

6.3.2 Training shall be delivered on a "just-in-time" basis as agreed between the Parties.

6.3.3 The Contractor shall provide initial IDENT1 training to the FPOs of Scotland. The Contractor shall provide further training on all new IDENT1 capabilities to the FPOs of Scotland.

6.4 Ongoing Training

6.4.1 The Contractor shall provide training in new capabilities to Bureau Trainers.

6.4.2 The Contractor shall provide a catalogue of additional training courses, which shall be optionally available to users and are additional to those already catered for in the Contractor's baseline, that shall include, but not be limited to:

(a) MIS/Audit—Advanced Courses

(b) Advanced Management of Livescan

(c) Livescan—Print Capture Quality

(d) Legacy Livescan/Custody Interface

(e) Generic Mark Camera Interface

(f) Palm Processing

(g) Serious Crime Cache

(h) Operational Response Database

(i) Identification Technology

6.4.3 The Contractor shall provide reasonable levels of training for the Authority and other approved third parties to facilitate the collection of Management Information.

6.4.4 The Contractor shall provide reasonable levels of training to Bureau managers to enable them to collect business metrics on Bureau performance.

6.4.5 The Contractor shall provide training at the following locations:

(a) Contractor facilities at Solihull.

(b) Onsite at Bureaux/within force.

(c) Ad hoc locations as mutually agreed upon between the Contractor and the Authority.

6.4.6 The Contractor shall provide any necessary additional equipment to carry out onsite training.

6.4.7 The Contractor shall provide qualified trainers to carry out user/system/support training under the Contract.

6.4.8 The Contractor's trainers shall have a combination of training and domain experience. The Contractor's trainers shall have appropriate training qualifications.

6.4.9 The Contractor will provide a temporary training system for Scotland, at or close to Glasgow, which will stay in place until TOR-SAFR.

6.5 Computer Based Training (CBT)

6.5.1 The Contractor shall work with the Authority to define the most appropriate CBT solution (as detailed in Schedule O:28 (**Documentation**); however, the Contractor shall provide the user with, at a minimum:

(a) Information screens

(b) An overview of processes

(c) Pictures of equipment

(d) Diagrams naming parts of the system

(e) Instructions on how to perform particular tasks

(f) Exercises to perform actions

(g) A review of what the user has done

(h) Feedback on performance

6.5.2 Development of the CBT shall be undertaken in conjunction with the Authority and shall be subject to the Test and Acceptance procedures defined in Schedule H (**Acceptance Procedures**).

6.5.3 CBT shall be accessible to users from their IDENT1 workstations through a web interface.

6.5.4 CBT shall be updated in line with system developments and changes.

6.6 Online Help and User Manuals

6.6.1 Users shall be provided with an online help facility at their workstations for assistance on performing normal operational tasks.

6.6.2 The Contractor will develop, in consultation with the Authority, User Manuals (as set out in Schedule O:24 (**Documentation**)) and an Operations and Maintenance Support Plan (as set out in Schedule O:58 (**Documentation**)) describing the use and operational processes of the Services and all aspects of the system.

6.6.3 All documentation and training material, including those set out in 6.6.2, shall be available through a web portal. The Authority shall be authorised to freely distribute documentation and training materials amongst parties authorised by the Authority.

6.7 Training Manuals

6.7.1 All courses developed by the Contractor shall include user guides and aides-memoirs, which shall be made available to students and/or to accredited force trainers delivering IDENT1 training (see Schedule O:25 (**Documentation**)).

6.7.2 The Contractor shall develop, in consultation with the Authority, training documentation that shall cover all aspects of the system (see Schedule O:23 and 29 (**Documentation**)).

6.7.3 Training Material shall be updated to reflect changes to the system (see Schedule O:26 (**Documentation**)).

6.7.4 All training documentation shall reflect the differences in terminology among Scotland and England and Wales.

6.7.5 Paper copies of training materials shall be provided in support of training courses run by the Contractor (see Schedule O:26 (**Documentation**)).

6.7.6 Electronic copies of training documentation shall be made available to the Authority and users so that additional copies can be produced locally, as required.

6.7.7 The Authority shall be provided with the opportunity to review in a timely manner all training documentation and course structure before they are released.

6.8 Livescan/EIU Training

6.8.1 The Contractor shall provide a training course with each EIU that is deployed to a Custody suite. Each training course shall accommodate up to eight students, who will then be accredited to provide cascade training to other custody suite staff.

6.8.2 The Contractor shall provide training in other EIUs when they are deployed. The Contractor shall provide an EIU training system at each of the regional training centres in Hendon, Durham, and Wyboston.

6.8.3 The training systems shall replicate the full system functionality available at the custody suite and will be updated with the most current software releases. The EIU

training system at each of the regional training centres will interact with the installed training systems for FPO training and mimic the functionality of the operational system.

6.8.4 The Contractor shall provide hardcopy training materials and user manuals to students attending courses run by the Contractor. Updates to user manuals will be provided to each custody suite. These materials will be made available in electronic format through the knowledge portal and will be available for reproduction by the Authority or other parties as approved by the Authority.

6.8.5 The Contractor shall develop, update, and maintain training and user manuals to be used at regional training centres. The Contractor will work with the Authority to produce the training materials and will obtain the Authority's approval of materials to be provided to users.

6.8.6 EIUs at custody suites shall support training of operational personnel in a training mode, which does not impact the operational system.

7 DEVELOPMENT

7.1 Development

7.1.1 The Contractor's development process shall conform to industry best practices and include, at a minimum:

(a) Developing software iteratively.

(b) Managing requirements.

(c) Visually modelling software.

(d) Using component architecture.

(e) Verifying software quality.

(f) Controlling changes to software.

7.1.2 The Contractor shall use Rational Unified Process (RUP) (in particular, RUP for Systems Engineering) or an equivalent established development process.

7.1.3 The Contractor's development process shall be mature, documented, and compliant with CMM.

7.1.4 The Contractor shall agree upon a Development Strategy with the Authority in accordance with Schedule O:9 (**Documentation**).

7.1.5 The Contractor, in conjunction with the Authority, shall carry out further analysis and development of the Functional Requirements to ensure that they are a complete and accurate representation of the user's then current needs.

7.1.6 The Contractor shall carry out performance modelling of the IDENT1 Service. The results from the performance modelling shall be considered in the development process during the Inception Phase .

7.1.7 The Contractor shall construct a conceptual model for the IDENT1 Service, using the existing NAFIS Services System and DOR Use Cases as a starting point see Schedule Q Part B (**System Description**).

7.1.8 The Contractor shall catalogue and classify the IDENT1 Services requirements in accordance with the requirements management approach defined by the Authority.

7.1.9 The Contractor shall use a compatible method for managing requirements and exchange requirements information with the Authority in a format suitable for importing, as defined by the Authority.

7.1.10 The Contractor shall work with the Authority and the user community to capture, validate, and verify new requirements emerging during the lifetime of the Services. Any new requirements will result in a change to the Services which shall be varied in accordance with Schedule L (**Change Control Procedure**).

7.1.11 The Contractor shall assist the Authority in analysing new requirements by carrying out impact assessments when appropriate in accordance with Schedule L (**Change Control Procedure**).

7.1.12 The Contractor shall conduct a Lifecycle Objective Milestone review.

7.1.13 The Contractor shall conduct a Lifecycle Architecture Milestone review.

7.1.14 The Authority shall make the final assessment on whether new requirements are to be progressed to development.

7.1.15 The Contractor shall provide and maintain a Software Development Plan that details all analysis, design, build, and deployment tasks based on the agreed-upon development strategy (as set out in Schedule O:32 (**Documentation**)).

7.1.16 The Contractor shall validate and enhance the business requirements to ensure that they have a firm basis for developing the system requirements.

7.1.17 The Contractor shall provide the analysis and design methods to be used during the development cycle, clearly stating how each product is to be produced and used during each stage to produce the final system.

7.1.18 The Contractor shall provide system development documentation for the IDENT1 Services to the Authority in RUP terms.

7.1.19 All software products shall be subject to formal Quality Review as described in the Programme Quality Plan (as set out in Schedule O:10 (**Documentation**).

7.1.20 The Contractor shall develop and agree upon quality criteria with the Authority during the planning stage.

7.1.21 The Contractor shall use system architecture principles to guide the development of the system architecture that shall be represented in a model in order to facilitate reviews between the Authority and the Contractor.

7.1.22 The Contractor shall provide the Authority with a System Architecture Model detailing the major hardware, software and network components of the IDENT1 Service (see Schedule O:43 (**Documentation**)).

7.1.23 The System Architecture Model shall clearly identify which components are existing infrastructure, which are COTS, and which are Contractor developed.

7.1.24 The System Architecture Model shall distinguish between functional and physical components.

7.1.25 The System Architecture Model shall clearly identify all major subsystems and describe their purpose.

7.1.26 The Contractor shall maintain the System Architecture Model during the term of the Contract and incorporate all enhancements and upgrades.

7.1.27 The Authority shall have the right to reuse information from the System Architecture Model for future systems development.

7.1.28 The Contractor shall provide the Authority with full access to all Data Models (conceptual, logical, or physical) produced for the Service (as set out in Schedule O:44 and 45 (**Documentation**)).

7.1.29 The Authority shall have the right to reuse information from Data Models in future systems development.

7.1.30 The Contractor shall use the procedures from the Quality Plan to ensure quality in software development.

7.1.31 The Contractor shall ensure that any developed code is produced according to the Quality Plan.

7.1.32 The Contractor shall agree upon escrow arrangements with the Authority, in accordance with Schedule B (**Conditions of Contract**), to cover all developed code, together with supporting design documentation and any proprietary technology necessary to make use of the code.

7.1.33 The Contractor shall document all interfaces and Application Programming Interfaces built for the Service in ICDs (as set out in Schedule O:46 (**Documentation**)).

7.1.34 The Authority shall have the right to share information contained in ICDs with third parties where integration with the IDENT1 Services is required.

7.1.35 The modelling notation used to communicate with the Authority during development shall be UML.

7.1.36 The Contractor's development environment shall be completely separate from the live and test environments.

7.1.37 The Contractor shall use a controlled process to move code, documentation, and data from the development environment through to the test and subsequently live environments.

7.1.38 The Contractor shall agree upon the choice of development tools with the Authority, taking into account compatibility with other Authority development work.

7.1.39 The choice of development tools shall be consistent with the IDENT1 Service Technical Architecture.

7.1.40 The Contractor shall establish, implement, and maintain a Business Process Engineering (BPE) capability, responsible for assisting the Authority's Fingerprint Service in the definition and the development of their business processes (see Schedule O:36 (**Documentation**)).

7.1.41 The Contractor shall provide evidence to the Authority that its BPE team has a proven process and methodology.

7.1.42 The Contractor shall work with the Authority to define business process design standards and procedures for implementation.

7.1.43 The Contractor shall work with the Authority to review the current processes to identify problems and issues that need to be addressed.

7.1.44 The Contractor shall work with the Authority to produce statements of new processes and to assist the Authority in the appropriate distribution and implementation.

7.1.45 The Contractor shall ensure that all workflow and business process design shall be provided within a workflow modelling tool.

7.1.46 The Contractor's IDENT1 system shall contain a workflow solution.

7.1.47 The Contractor's workflow solution shall conform to relevant industry standards.

7.1.48 The workflow modelling tool shall be capable of demonstrating that the proposed solution is capable of delivering the overall performance objectives and how changes in workload shall impact response times and throughput.

7.1.49 The workflow modelling tool shall be able to model a workflow that contains a mix of manual, semi-automated, and automated functions.

7.1.50 The workflow modelling tool shall be able to measure total process times of minutes or hours—consisting of individual processes that take seconds or minutes—and total throughput volume under typical demand conditions and peak demand conditions.

7.1.51 The workflow modelling tool shall be provided through commercially available workflow management products and not through custom-built solutions.

7.1.52 The Contractor shall provide the Authority with justification for COTS products chosen (as set out in Schedule O:41 (**Documentation**)).

7.1.53 The Contractor shall seek the approval of the Authority before purchase of COTS products for use in the delivery of Service.

7.1.54 The Contractor shall document COTS software products and version numbers that are required, incorporated, or included as part of its solution for delivery of the Service (as set out in Schedule O:42 (**Documentation**)).

7.1.55 The Contractor shall document any ratings, certifications, and industry standards achieved by the COTS software.

7.1.56 The Contractor shall provide documentation describing all changes made to a COTS software product implemented as part of the Service.

7.1.57 The Contractor shall propose and agree with the Authority on a software configuration management process for the Service and document this in accordance with Schedule O:34 (**Documentation**).

7.1.58 The Contractor shall be permitted to choose appropriate tools to support the software configuration management process subject to approval by the Authority.

7.2 Usability

7.2.1 The Contractor shall carry out any necessary rework resulting from usability testing to meet Contract requirements prior to implementing the HCI (as set out in Schedule O:70 (**Documentation**)).

7.2.2 The Contractor shall design the Service to maximise the efficiency and effectiveness of users while providing a safe and comfortable work environment.

7.2.3 The Contractor shall ensure that the usability requirements for the Services System apply to all applications and equipment accessible to the user.

7.2.4 The Contractor shall develop, document, and use a User Centred Design process for the development of the Service.

7.2.5 The Contractor shall describe its approach to User Centred Design for the Services in the Programme Initiation Review Documentation.

7.2.6 The Contractor shall include User Centred Design activities in the development plans.

7.2.7 The Contractor shall include user representation from different groups of users in the User Centred Design process.

7.2.8 The Contractor shall document usability requirements during the design phase so that the system can be tested for conformance to these requirements.

7.2.9 The Contractor shall make available such documentation produced to support the usability of the Service to the Authority (as set out in Schedule O:48 (**Documentation**)).

7.2.10 The IDENT1 Services shall continue to be evaluated on a reasonable basis by the Contractor after implementation to ensure that it continues to meet usability requirements.

7.2.11 The Contractor shall on a reasonable basis improve the usability of the system for bureau users by using a User Centred Design process in which the usability requirements will be identified, the system evaluated against these requirements, and the system redesigned to meet the usability requirements through an iterative process.

7.2.12 The Contractor shall on a reasonable basis identify and analyse the types of environment and tasks in which mobile access to the IDENT1 Service is required in order to design HCIs and equipment that address the specific usability needs of users with mobile access to the system.

8 TEST AND ACCEPTANCE APPROACH

8.1 The Contractor shall present a Test and Acceptance Strategy to the Authority at the project initiation event. All testing will be done in accordance with this strategy.

8.2 The Contractor's Test and Acceptance Strategy shall support delivery of new functionality in incremental releases.

8.3 The Contractor shall be responsible for the performance of all validation and verification activities, including formal and informal testing of functionality, performance, usability, backward compatibility, PNC, and regression tests.

8.4 The Authority shall be entitled to attend all test events at its discretion, and the Contractor shall reasonably facilitate such attendance.

8.5 The Contractor shall incorporate users and user opinions in its verification and validation activities.

8.6 Where appropriate and to retain benefits from the investment in the NAFIS Services, the Contractor shall, at the Authority's discretion, reuse test scripts, processes, data, and test beds used in the development and provision of the NAFIS Services.

8.7 The Contractor shall collect metrics to use in improving the development and test process in accordance with Schedule H (**Acceptance Procedures**).

8.8 The Contractor shall at its discretion and on a reasonable basis develop automated test tools to reduce the time and cost of regression testing.

8.9 The Contractor shall use IEEE 829 as a framework for test documentation in accordance with Schedule O:1, 2 and 4 (**Documentation**).

8.10 The Contractor shall identify and comply with the procedures used in recording the results of other verification activities, such as peer review, inspections, audits and analysis, and unit and integration testing, as described in Schedule H (**Acceptance Procedures**).

8.11 Subject to Schedule H (**Acceptance Procedures**), the Contractor shall migrate the current NAFIS Requirements Database and all associated verification data to an appropriate tool agreed upon between parties. The Contractor shall use test material used for the NAFIS Services to test IDENT1 requirements that map directly to already verified NAFIS requirements.

8.12 The Contractor shall perform prerelease defect and regression testing to ensure that existing functionality has not been impacted as described in Schedule H (**Acceptance Procedures**).

8.13 The Contractor's testing cycle shall include development tests, integration tests, informal and formal dry run tests, and formal acceptance tests.

8.14 The Contractor shall conduct a formal Test Readiness Review (TRR) (as set out in Schedule O:6 (**Documentation**)) with the Authority before proceeding with formal acceptance testing, as described in Schedule H (**Acceptance Procedures**). This TRR will result in the production of minutes (as set out in Schedule O:3 (**Documentation**)).

8.15 The Contractor shall hold a Product Acceptance Review at the conclusion of acceptance testing, as described in Schedule H (**Acceptance Procedures**).

8.16 The Contractor shall hold Operational Readiness Review's (ORR's) to affirm that releases are ready for deployment, as described in Schedule H (**Acceptance Procedures**).

8.17 The Contractor shall maintain configuration management of all test documents against the project baseline.

8.18 The Contractor's test programme shall ensure that test procedures are subject to peer review before release, as described in Schedule H (**Acceptance Procedures**).

8.19 The Contractor shall support upon the Authority's request for specific program requirements, tailoring of the standard testing processes. The Contractor shall conduct and document acceptance testing of subcontractor-delivered products. The Contractor's processes and procedures shall be consistent with those used in the overall Contractor's product life cycle.

8.20 Unless otherwise agreed with the Authority for all system upgrades, the Contractor shall as a minimum conduct regression and performance testing of existing capabilities.

8.21 For the Palms Transition Project, the Contractor shall perform the following tests: demonstration and performance, integration and formal dry runs, regression, validation and acceptance.

8.22 Evidence of unit and integration testing shall be recorded in the programme filing system, and shall be made available to the Authority, upon request.

8.23 The Contractor shall develop and maintain regression test procedures as described in Schedule H (**Acceptance Procedures**).

8.24 The Contractor shall conduct, where the Authority deems appropriate, other testing, including load testing scripts, external (e.g., PNC, Police Immigration Fingerprint Exchange), backward compatibility, switchover, and defect testing as described in Schedule H (**Acceptance Procedures**).

8.25 Configuration Management and QA roles and responsibilities in the Test and Acceptance Process shall be defined in the respective Configuration Management and QA plans produced in accordance with Schedule O:10 and 34 (**Documentation**).

8.26 New releases shall be made available to users on the integration test bed at Hendon or the secondary site, to allow users and the Contractor user support group to become familiar with and appraise the new functionality as described in Schedule H (**Acceptance Procedures**). User comments shall be incorporated into the test report.

8.27 The Contractor shall develop prototypes and demonstrations, where it deems appropriate as described in Schedule H (**Acceptance Procedures**).

8.28 The Contractor shall establish and maintain a UK prototyping lab to support systems engineering activities, as described in Schedule H (**Acceptance Procedures**). A link to the development facility in the US shall be provided.

8.29 The Contractor shall conduct checkout testing at the initially deployed bureaux by providing user support at each of these bureaux, as described in Schedule H (**Acceptance Procedures**).

8.30 The Contractor shall seek Authority approval, which shall not be unreasonably withheld before conducting any testing involving the operational system; except where otherwise agreed upon between the parties, such testing will be performed in a manner that will have no impact on system performance as specified in Schedule F (**Service Level Requirements**).

8.31 The Contractor shall analyse all Services requirements to determine at which stage or stages of the Contract they can be most logically verified and included in the next Stage Plan for approval (as set out in Schedule O:18 (**Documentation**)).

8.32 Functional requirements, such as HCI, critical to project success shall be verified with user evaluation, as described in Schedule H (**Acceptance Procedures**).

8.33 The Contractor shall tailor test procedures and resources to the type of activity performed for each phase of testing and the functionality in the current release of the software as agreed with the Authority (as set out in Schedule O:2 (**Documentation**)).

8.34 The Contractor shall use test tools as agreed with the Authority to support test and acceptance activities.

8.35 The Contractor shall establish and maintain a controlled test environment that mirrors the operational system, including bureau and central configurations as described in Schedule H (**Acceptance Procedures**).

8.36 The Contractor shall maintain test data comprising marks, ten prints, and palms. Test data for the IDENT1 Services shall be largely derived from the test data maintained for the NAFIS Services and data provided to the Contractor by the Authority.

8.37 The Contractor shall maintain test data to support testing of new capabilities as described in Schedule H (**Acceptance Procedures**).

8.38 Insofar as it is within the Contractor's control, the Contractor shall maintain a live connection with the PNC in the test bed to support PNC testing on an as-required basis. Similar functionality shall be built to support other external interfaces.

8.39 The Contractor shall conduct testing of message-based interfaces through scripts simulating the target systems.

8.40 The Contractor shall maintain test traceability, including test procedures, test scripts, requirements, and verification methods as described in Schedule H (**Acceptance Procedures**).

8.41 The Contractor shall maintain multiple test beds to support IDENT1 test and acceptance activities.

8.42 As part of the acceptance test plan, the Contactor shall obtain the Authority's approval for test locations, which approval shall not be unreasonably withheld.

8.43 The Contractor shall include testing of the Training Bureau functionality as part of regression testing.

9 CAPACITY MANAGEMENT

9.1 The Contractor shall deliver a Capacity Management Plan as set out in Schedule O:64 (**Documentation**). They shall implement the Capacity Management Process as part of its Systems Engineering process. The Capacity Management Plan shall be ITIL compliant. The Capacity Management Plan shall address the full range of IDENT1 Services, including central site(s), bureaux systems, and remote EIUs. The Capacity Management Plan shall also address the communications infrastructure and system interfaces.

9.2 The Capacity Management Process shall address the following elements:

9.2.1 UPSs for IDENT1 kit at the Central Site and all bureaux locations.

9.2.2 Monitoring of system resource utilisation.

9.2.3 Trend analysis.

9.2.4 Identification of elements of the configuration that could be tuned for improved resource utilisation.

9.2.5 Maintenance of capacity management data on key system resources.

9.2.6 Forecast capacity and delivered capacity against actual usage.

9.2.7 Demand management activities.

9.2.8 System modelling that addresses capacity issues and planning.

9.3 The Contractor shall designate a capacity manager who shall interface with the Authority's capacity manager. The Contractor's capacity process shall be managed under the Systems Engineering functional area.

9.4 The capacity management process shall include inputs from engineering modelling and performance assessments, as well as operational supportability considerations. The capacity management process shall be documented in the Operations and Maintenance Support Plan.

9.5 The capacity management process shall include system monitoring capabilities. The Authority shall be provided access to the system monitoring facilities via a web portal interface.

9.6 The Contractor shall implement appropriate tools to record and analyse historic capacity and usage at a business, service, and resource level. The Authority shall be provided with access to the tools and data.

10 SECURITY

10.1 The Contractor shall implement and deliver a Security Management Process that ensures that the Services meet the IDENT1 operational security requirements. The Security Management Process shall be ISO 17799 compliant. The Contractor shall be responsible for full system security, including the WAN. The Contractor shall be fully responsible for implementing system and component changes and enhancements required to meet system operational security goals.

10.2 The Contractor's Security Management Process shall incorporate key elements of the Contractor's existing design and support structure, including:

10.2.1 A Chief Engineer responsible for ensuring that security attributes are incorporated into the overall software and system design at every step of the systems engineering and implementation process.

10.2.2 An accredited test and development facility connected to the IDENT1 WAN with CAPS-approved encryption.

10.2.3 A single onward connection at each central site to the CJX, providing a clear security boundary between IDENT1 and external users and systems.

10.2.4 The use of LDAP and Simple Authentication and Security Layer for user authentication.

10.2.5 The use of TACACS+ and RADIUS for remote user access and system component access.

10.2.6 Flowdown of security requirements to suppliers such as the WAN provider or the maintenance provider.

10.2.7 Multiple test beds to evaluate new products and component suitability.

10.3 The Contractor's security management activities shall:

10.3.1 Review and analyse security requirements, through its systems engineering process.

10.3.2 Review impacts to business functions arising from security issues, including identifying critical system security components (as set out in Schedule O:57 (**Documentation**)).

10.3.3 Arrange annual system security audits by external parties and IT health checks annually or at the request of system accreditors.

10.3.4 Form Computer Emergency Response Teams (CERTs) in response to security incidents.

10.3.5 Review access lists of users and administrators on a monthly basis to ensure appropriate access privileges and group assignments.

10.3.6 Review of audit and accounting logs commensurate with the Protective Markings.

10.3.7 Maintain and update a Security Management Plan meeting the requirements of ISO 17799. This plan shall include periodic vendor assessments of current and new products and technologies applicable to security. The Security Management Plan shall be made available for the Authority for review and comment.

10.3.8 Implement a Security Awareness Training Programme to provide annual documented training to all users (as set out in Schedule O:30 (**Documentation**)).

10.4 The Contractor shall designate a System Security Officer (SSO) who shall interface with the Authority's SSO for IDENT1. The SSO shall have overall responsibility for the security operations of the IDENT1 programme. The Contractor's SSO shall report to the Contractor's Programme Director. Serious security issues shall be escalated to the Contractor's Chief Engineer and/or the Contractor's Programme Director. The SSO shall report any security breaches to the Programme Director and to UNIRAS if appropriate.

10.5 The system security status shall be reported on a monthly basis. The Authority shall be provided with reasonable access to MIS and system audit logs to assist in analysis of system security performance.

10.6 The Contractor's Security Management Process shall be an integral aspect of its overall systems engineering activities to ensure that security is considered within the IDENT1 life cycle. The Security Management Process shall be documented in the Operations and Maintenance Support Plan.

10.7 The Contractor's Security Management Process shall include mechanisms for delivering changes to the system resulting from security reviews and CERT findings.

10.8 The Contractor's Security Management Process shall include mechanisms for communicating security incidents to the Authority and to users.

11 FUTURE VISION

11.1 The Contractor shall design the IDENT1 system architecture to support a Strategic Identification Services Platform (SISP) that provides the capability to incorporate new functionalities. At a minimum, the capability shall be provided to incorporate the following new functionalities:

11.1.1 Multi-Modal Biometrics

11.1.2 Integrated Feature Management

11.1.3 Multi-Classifier Systems

11.1.4 Facial Image Collection and Recognition

11.2 The Contractor's system architecture shall support algorithm fusion. The architecture shall support new AFR fusion algorithms and fusion of algorithms across multiple biometrics.

11.3 The Contractor's IDENT1 architecture shall provide the capability to link and integrate with external systems within the criminal justice environment.

11.4 The Contractor's IDENT1 architecture shall be designed so as to enable the provision of capability in the future for IDENT1 users to make use of identification information held on other systems.

11.5 The Contractor's IDENT1 architecture shall be designed so as to enable the support of new delivery mechanisms to provide information at the point of need. The Contractor's IDENT1 architecture shall support future locations and new roles within the identification environment.

11.6 The Contractor shall maintain active membership with such international biometrics organisations and standards bodies as it deems appropriate.

11.7 The Contractor shall work on a reasonable basis, in conjunction with the Authority, to address standards and implementation issues to support IDENT1 strategic identification services.

11.8 The Contractor shall provide BPE teams to develop use cases for new functionality. The Contractor's BPE team shall include relevant systems engineering, business process, change management, and operational user experience.

11.9 The Contractor shall develop a strategic plan that addresses the strategy for introducing changes to the IDENT1 Services System. The Contractor's strategic plan shall consider and complement PITO's Biometric Technology Roadmap and demonstrate potential future benefits of IDENT1 in terms of systems and services. The Contractor's strategic plan shall be reviewed and updated, as appropriate, on an annual basis.

11.10 The Contractor shall employ such prototyping and piloting of new functionality as agreed with the Authority within the Contractor's facilities to facilitate user and stakeholder feedback and reduce implementation risk.

11.11 The Contractor shall maintain an independent research and development (R&D) programme associated with strategic identification technologies. The Contractor shall provide results of R&D activities to the Authority.

11.12 The Contractor shall within its discretion and planning host an annual identification technology forum to provide technical vision in the areas of biometrics, display concepts, and

security in relationship to the IDENT1 services strategic plan. The forum shall include senior managers and technologist from the Contractor's team. The Authority shall be invited to participate in this forum at the Authority's discretion.

11.13 The Contractor shall deliver technology refreshes of the IDENT1 Services between FOC and EOC to support the agreed-upon Schedule F (**Service Level Requirements**) upgrades and forecasted capacity increases.