

# An Garda Síochána

Oifig Saorála Fáisnéise,  
An Garda Síochána, Teach áth Luimnigh,  
Lárionad Gnó Udáras Forbartha Tionscail,  
Baile Sheáin , An Uaimh,  
Contae na Mí.  
C15 ND62



Freedom of Information Office,  
An Garda Síochána, Athlumney House,  
IDA Business Park,  
Johnstown, Navan,  
Co Meath.  
C15 ND62

Teileafón/Tel: (046) 9036350



Láithreán Gréasain/Website:  
[www.garda.ie](http://www.garda.ie)

Ríomh-phoist:/Email: [foi@garda.ie](mailto:foi@garda.ie)

## Re: Freedom of Information Request FOI-000062-2021 Request Part Granted

*Dear*

I refer to your request, dated and received on 12<sup>th</sup> February, 2021 which you have made under the Freedom of Information Act 2014 (FOI Act) for records held by An Garda Síochána.

Part 1(n) of Schedule 1 of the FOI Act states that An Garda Síochána is listed as a partially included agency "*insofar as it relates to administrative records relating to human resources, or finance or procurement matters*". Therefore, only administrative records that relate to human resources, finance or procurement shall be considered.

Your request sought:

*In accordance with section 12 of the Freedom of Information Act 2014, I wish to request*

- *a breakdown of the support and maintenance services costs paid to Accenture as per Q3 Purchase orders.*
- *any tenders relating to the same.*

I wish to inform you that I have decided to part grant your request on the 12<sup>th</sup> April 2021.

The purpose of this letter is to explain that decision.

### **1. Findings, particulars and reasons for decision**

On receipt, your request was forwarded to the Information & Communications Technology, Finance and Procurement Sections of An Garda Síochána who in turn provided a number of records.

Firstly, I must inform you of the provisions of Section 42 of the Freedom of Information Act wherein:

**Restriction of Act**

42. *This Act does not apply to—*

*(b) a record held or created by the Garda Síochána that relates to any of the following:*

*(v) the Security and Intelligence Section;*

Section 42 of the Act is a mandatory exemption and I am obliged to refuse the release of any records relating to Security & Intelligence Section.

Having examined the remaining records, I wish to advise as follows. Part 1 of your request sought “*a breakdown of the support and maintenance services costs paid to Accenture as per Q3 Purchase orders*”. The table below details a breakdown of support and maintenance costs paid.

PO Number	Payee	Amount	Maintenance	Support
197780	Accenture	€132,000.00	€132,000.00	
198477	Accenture	€185,990.00	€185,990.00	
198757	Accenture	€275,876.50		€275,876.50
198848	Accenture	€612,280.00		€612,280.00

In respect of part 2 of your request seeking “*any tenders relating to the same*”, I am enclosing herewith copies of same. Redactions have been applied to a number of these documents and schedules are attached outlining the redactions. The redactions are applied in accordance with the terms of the Freedom of Information Act.

Part 1(n) of Schedule 1 of the FOI Act states that An Garda Síochána is listed as a partially included agency “*insofar as it relates to administrative records relating to human resources, or finance or procurement matters*”. Therefore, only administrative records that relate to human resources, finance or procurement shall be considered. Records relating to operational policing matters are outside the scope of the FOI Act insofar as it relates to An Garda Síochána.

I am refusing the release of certain information contained in the attached records pursuant to Section 36(b) and (c) of the FOI Act which states:

**Commercially sensitive information**

36. (1) *Subject to subsection (2), a head shall refuse to grant an FOI request if the record concerned contains—*

- (b) financial, commercial, scientific or technical or other information whose disclosure could reasonably be expected to result in a material financial loss or gain to the person to whom the information relates, or could prejudice the competitive position of that person in the conduct of his or her profession or business or otherwise in his or her occupation, or*
- (c) information whose disclosure could prejudice the conduct or outcome of contractual or other negotiations of the person to whom the information relates.*

I am satisfied that the release of certain redacted information contained within the attached records would prejudice the competitive position of the supplier by making their pricing structure publically known. This information therefore is commercially sensitive in accordance with the provisions of Section 36 of the Act

I am cognisant of the fact that the release of information under the Act is, in essence, a release to the public at large. The pricing structure of the supplier with regard to services provided to An Garda Síochána is not known to competitors or the public in general. If the records were made available to you it is reasonable to expect that it would prejudice the ability of the supplier to compete in other contracts or negotiations in the future as competitors would be aware of their pricing structure.

I am of the view that the release of the pricing structure could reasonably be expected to result in a material financial loss by the supplier as it could prejudice their competitive position in the conduct of their business. The placing of these pricing structures into the public domain could also reasonably be expected to give a competitive advantage to other companies seeking similar contracts with public bodies.

Furthermore the supplier's current customers may become aware of a potential difference in pricing structures being offered to An Garda Síochána which could prejudice any current or future negotiations with these customers.

Therefore, I am refusing this part of your request under the provisions of section 36(1)(b) & 36(1)(c) as it seeks commercially sensitive information.

### **Public Interest Test**

There is a Public Interest Test associated with section 36 of the FOI Act whereby my decision must be made having fully considered the public interest relevant to this request.

I have considered the public interest issues which arise in this case and have taken account of the following factors in favour of release:

- Ensuring openness and transparency of organisational functions to the greatest possible extent.
- The public interest in members of the public exercising their rights under the FOI Act.
- That there is more than just a transitory interest by the public in this information being released.
- The right to commercial confidentiality is outweighed by the needs of the public regarding the expenditure of public funds by a public body.

In considering the public interest factors which favour withholding the records I have taken account of the following:

- Allowing a public body to hold commercial information without undue access by members of the public.
- The best course of action which is in the public interest with regard to these records.
- That An Garda Síochána can conduct its business with external contractors in a confidential manner.

- That there is a reasonable and implied expectation by contractors that financial information pertaining to services provided will be held in a confidential manner.
- That there is no overriding public interest that outweighs the right to privacy by an individual or in this case the financial activities of a service provider.

Having balanced the public interest factors both for and against the release, I decided that the public interest in preserving the information and the reasonable expectation that information can be maintained by An Garda Síochána without prejudicing future financial endeavors by external service providers outweighs the public interest which would be served were the records released to you.

I am also refusing the release of certain information contained in the attached records pursuant to Section 37 of the Act which states:

*37 (1) Subject to this section, a head shall refuse to grant an FOI request if in the opinion of the head, access to the record concerned would involve the disclosure of personal information (including personal information relating to a deceased individual).*

Personal information is defined within the FOI Act as:

*"personal information" means information about an identifiable individual that, either*

*(a) would, in the ordinary course of events, be known only to the individual or members of the family, or friends, of the individual, or*

*(ix) a number, letter, symbol, word, mark or other thing assigned to the individual by an FOI body for the purpose of identification or any mark or other thing used for that purpose*

I am refusing to provide certain information contained within enclosed records as I believe that the release of this information, which is specific to an individual(s), be released into the public domain.

There is a Public Interest Test applicable to section 37 of the FOI Act.

### **Public Interest Test**

As per section 37 of the FOI Act I have considered the public interest issues which arise in this case and have taken account of the following factors in favour of release:

- Ensuring openness and transparency of organisational functions to the greatest possible extent,
- The public interest in members of the public exercising their rights under the FOI Act,
- The right to privacy is outweighed by the needs of the public.

In considering the public interest factors which favour withholding the records I have taken account of the following:

- Allowing a public body to hold personal information without undue access by members of the public,
- The public interest is not best served by releasing these records,
- That there is no overriding public interest that outweighs the individual's right to privacy.

A public interest test was carried out when considering the release of the personal information but having balanced the factors both for and against the release, I decided that the public interest in preserving the personal information and the reasonable expectation that information can be maintained in a confidential manner by An Garda Síochána outweighs the public interest which would be served were the records released to you in their entirety.

## **2. Right of Appeal**

In the event that you are not happy with this decision you may seek an Internal Review of the matter by writing to the address below and quoting reference number **FOI-000062-2021**.

*Freedom of Information Office, An Garda Síochána, Athlumney House, IDA Business Park, Johnstown, Navan, Co. Meath C15 ND62*

Please note that a fee applies. This fee has been set at €30 (€10 for a Medical Card holder). Payment should be made by way of bank draft, money order, postal order or personal cheque, and made payable to Accountant, Garda Finance Directorate, Garda Headquarters, Phoenix Park, Dublin 8.

Payment can be made by electronic means, using the following details.

**Account Name:** An Garda Síochána Imprest Account

**Account Number:** 30000302

**Sort Code:** 951599

**IBAN:** IE28DABA95159930000302

**BIC:** DABAIE2D

**You must ensure that your FOI reference number (FOI-000062-2021) is included in the payment details.**

You should submit your request for an Internal Review within 4 weeks from the date of this notification. The review will involve a complete reconsideration of the matter by a more senior member of An Garda Síochána and the decision will be communicated to you within 3 weeks. The making of a late appeal may be permitted in appropriate circumstances.

Please be advised that An Garda Síochána replies under Freedom of Information may be released in to the public domain via our website at [www.garda.ie](http://www.garda.ie).

Personal details in respect of your request have, where applicable, been removed to protect confidentiality.

Should you have any questions or concerns regarding the above, please contact me by telephone at (046) 9036350.

Yours sincerely,



\_\_\_\_\_  
**PAUL BASSETT**  
**FREEDOM OF INFORMATION OFFICER**

12<sup>th</sup> APRIL 2021.

Requester Name:

Accenture MIMS Phase 3b - Major Investigations Dec 2015

File FOI-000062-2021

Page No	Description of Document	Deletions	Relevant Section of FOI Acts	Reason for Redaction	Decision Maker's decision
1	Corr from Exec Director ICT to Head of IT Planning 16/12/2015	0			Grant
2	Form of Notification to Activate	0			Grant
3	Project Initiation Document Cover Page	0			Grant
4-6	Table of Contents/Document Control	1	Section 37(1)	Personal Information	Part Grant
7	Introduction	0			Grant
8-22	Scope & Key Requirements	11	Part 1(n) of Schedule 1	Out of Scope	Part Grant
22-26	Proposed Solution	1	Part 1(n) of Schedule 1	Out of Scope	Part Grant
27-28	Project Plan & Control Mechanisms	0			Grant
29-31	Costs	7	Section 36(1)	Commercially Sensitive Information	Part Grant
32-36	Project Organisation	1	Section 37(1)	Personal Information	Part Grant
37-39	Key Assumptions	7	Part 1(n) of Schedule 1	Out of Scope	Part Grant
40-45	Control Mechanisms	1	Section 37(1)	Personal Information	Part Grant

# An Garda Síochána

Stiúrthóir Feidhmiúcháin  
Faisnéis & Cumarsáid Teicneolaíocht  
Ceanncheathrú An Garda Síochána  
Páirc on Fhionnuisce  
Baile Átha Cliath 8  
D08 HN3X



Executive Director  
Information & Communications Technology  
Garda Headquarters  
Phoenix Park  
Dublin 8  
D08 HN3X

Teileafón/Tel: (01) 6661451  
Facs/Fax: (01) 6661659

Láithreán Gréasain/Web Site: [www.garda.ie](http://www.garda.ie)  
Ríomh-phoist/E-mail: [Liam.Kidd@garda.ie](mailto:Liam.Kidd@garda.ie)

Bí linn/Join us  

---

**ICT\_4-467342/15**

**Mr. Aeneas Leane**  
**Head of IT Planning**

**Re: MIMS Phase 3B – Major Investigations – Project Initiation Document**

---

With reference to the above, please find attached signed Project Initiation Document for MIMS Phase 3B.

  
\_\_\_\_\_  
**Liam Kidd**  
**Executive Director of ICT**

**16** December, 2015





### FORM OF NOTIFICATION TO ACTIVATE PHASE

This is a notice for the purposes of Clause 3.5 of the Agreement made between the Commissioner of An Garda Síochána ("the Client") of the one part and Accenture of the other party on 20th day of December, 2010. The Commissioner **HEREBY NOTIFIES** Accenture that she wishes to activate the Phase and attendant Services detailed in the attached Project Initiation Document, reference number \_\_\_\_\_.

Dated: 16.12.2015

Signed: *Siobhán Widdell*  
Client's Project Manager  
An Garda Síochána  
Garda Headquarters  
Phoenix Park  
Dublin 8

To:

**Accenture Project Manager**

1 Grand Canal Square,  
Grand Canal Harbour,  
Dublin 2

**Major Investigations Management Systems**

**MAJOR INVESTIGATIONS MANAGEMENT SYSTEMS**

**M.I.M.S.**

**Phase 3b - Major Investigations**

**PROJECT INITIATION DOCUMENT**

**Version 1.4**

## TABLE OF CONTENTS

1. Introduction.....	6
2. Scope of Services and Key Requirements.....	7
2.1 Proposed Solution.....	21
2.2 Approach to Work.....	21
2.3 Security Arrangements.....	25
3. Project Plan and Control Mechanisms.....	26
3.1 Project Plan.....	26
3.2 Deliverables.....	27
4. Costs.....	28
4.1 Phase 3b Services Costs.....	28
4.2 Phase 3b Hardware and Software Costs.....	29
4.3 Reconciliation of Actual Costs against Estimated Costs.....	30
5. Project Organisation.....	31
5.1 Governance.....	31
5.2 Key Assumptions.....	35
5.3 Key Dependencies on An Garda Síochána.....	37
5.4 Exclusions.....	38
6. Formal Acceptance.....	38
6.1 Control Mechanisms.....	39
6.2 Progress Reporting.....	39
6.3 Change Control.....	39
6.4 Quality.....	39
6.5 User Acceptance Testing.....	40
7. Risk Management.....	41

**0.1 Prepared By**

Joe Taaffe

**0.2 Reviewed By**

Name	Role
Liam Kidd	Executive Director of ICT
Aidan Glacken	Chief Superintendent STO
Denis Ferry	Superintendent ICT STO
Aeneas Leane	Principal Officer IT Planning
Pat Ryan	Superintendent IT Operations
[REDACTED]	Accenture Account Manager

### 0.3 Documentation Control

During the course of the Project, it may be necessary to issue amendments or clarifications to parts of this document. This form must be updated whenever changes are made. Material changes to the Project Initiation Document ("PID") are subject to the approval of the governing Programme Board or as may be agreed in writing between the parties as per the change control mechanism outlined in Section 19 of the Agreement and as more particularly set out in Section 6.3 of this document. This PID is hereby incorporated into the Agreement.

Version	Section	Summary of Change	Prepared By	Date
0.1	All	Created	Joe Taaffe	09/06/2015
1.1	All	Finalised draft version	Joe Taaffe	13/10/2015
1.4	All	Updated following CSSO review	Joe Taaffe	15/12/2015

## 1. Introduction

This PID is executed by the Parties for the purposes of clause 3.5 of and governed by the ICT Services Agreement between the Commissioner of An Garda Síochána and Accenture dated 20<sup>th</sup> December 2010 ("Agreement"). All capitalised terms used herein shall have the meaning set out in the Agreement, unless otherwise indicated herein. References to "AGS" shall be a reference to the Client.

This PID outlines the scope of the services required for the design, build and implementation activities for Phase 3b of the Major Investigations Management System (MIMS) – Major Investigations (referred to as "Investigations Management system" in this PID). The objective of Phase 3b is to develop a single Investigations Management system for An Garda Síochána ("AGS") that will replace the manual, paper based process by which investigations are currently managed.

MIMS Phase 3b has been identified as a high priority initiative within An Garda Síochána's Policing & Security with TRUST Transformation Programme and will be the responsibility of one of the four newly established Programme Boards. For clarity, instructions and notices to Accenture will be in accordance with the provisions of the Agreement.

It should be noted that after the implementation of Phase 3b, it is intended that the MIMS Project will be delivered using a phased implementation approach to enable new functionality and technology to be developed and delivered in further phases, as follows:

- Phase 3a - Document and Content Management and Search for Major Investigations;
- Phase 4 - Enterprise Search;
- Phase 5 - Exhibit Tracking;
- Phase 6 - Investigative Analysis.

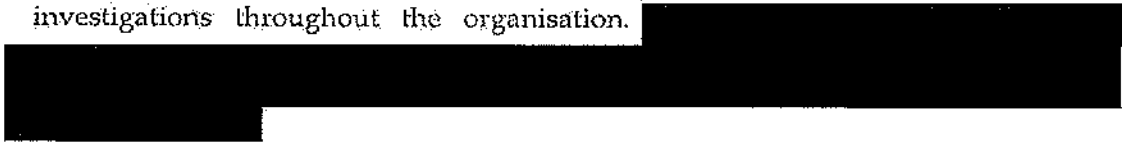
All of the aforementioned Phases (3a, 4, 5 and 6) are outside the scope of this PID. However, it is recommended that Phase 3a be delivered in parallel to allow the

intended integration of the Investigations Management system with the Enterprise Content Management system. Otherwise, the future integration of the Investigations Management system and the enterprise content management system may involve additional cost.

## 2. Scope of Services and Key Requirements

The key objective of Phase 3b is to implement a single Investigations Management system which will be used to manage the conduct of an investigation, tracking tasks, events and decisions. This system will integrate closely with the Document and Content Management and Search for Major Investigations and Exhibits Tracking System Components and other Garda IT systems such as PULSE. The introduction of this system into what is currently a paper based process will reduce effort, and greatly improve the effectiveness and usefulness of information gathered.

The main objectives of the Investigations Management system is to support An Garda Síochána manage activities completed as part of an investigation, maintain a full history of the chain of events in an investigation, information gathered, decisions made and actions undertaken. The Investigations Management system will integrate with the PULSE system ensuring a single view of information linked to investigations throughout the organisation.



The Provisions of Schedule A-Phase 3b: Major Investigations govern the provisions of this PID and are the point of reference in the detail descriptors set out below.

The Services delivered during this Phase are:-

1. Project mangement
2. Implementation Planning
3. Requirements Definition
4. Systems Testing
5. Systems Installation and Commissioning
6. Trtaining
7. End of Phase Report

The Investigations Management system will deliver the following functionality:


- Provide a unique identifier for each item linked to an investigation through the creation of entities in the investigation system. [REDACTED]
- Retain a full audit trail of all changes made to the entities, documents and records in an investigation. Thus a full audit trail of all activities associated with an investigation can be provided at any time.
- Allow for the attachment of files related to the investigation such as witness statements, charge sheets and video. This will be facilitated by the integration of an Enterprise Content Management system (ECMS). This is covered under MIMS Phase 3a. The parties acknowledge that this integration with ECMS cannot be delivered without certain elements of MIMS Phase 3a being completed.
- Provide investigation search facilities based on different criteria such as ID, content type, location etc.
- Provide a comprehensive reporting solution regarding the management of investigations. Standard reports will be created such as a "bingo card" report, disclosure report, final report for the DPP summarising the key details of the investigation and provide listings of key events, interviews, statements etc. Ad-hoc reports will also be possible.
- Provide integration with the Enterprise Content Management system providing access to all objects associated with a given investigation.

The Investigations Management system will address the following detailed requirements outlined in the Agreement:

#### Administrative Functions

- The system must allow a user with the appropriate privileges to set-up and manage a taxonomy of jobs based on the investigation classification type.





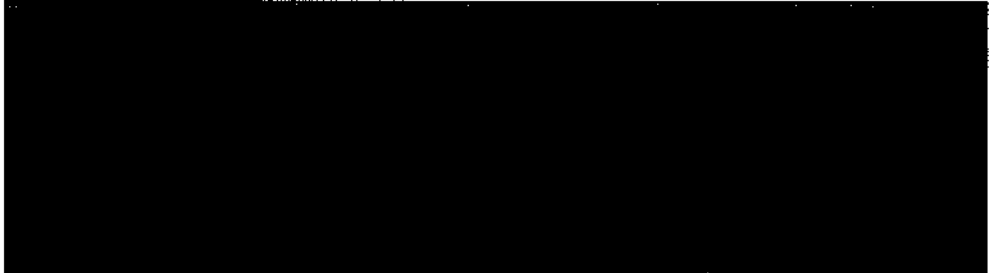
- The system must allow the set-up of different roles, for example book person, exhibits officer, questionnaire members, investigator and typists. Each role must be assigned different privileges in the system appropriate to the functions they must carry out. These roles must also be restricted to specific investigations.
- 

### Major Investigation Creation

- The system must provide the functionality to allow a user with the appropriate privileges to create and update an investigation record in the system.
- The system must automatically assign a unique identifier to the investigation.
- The system must allow the user to assign a code name to the investigation.



- The system must allow a user to select the appropriate classification for the investigation from a list that is stored in the system. This will classify the crime.
- The system must allow the status of an investigation to be updated and tracked.

- The system must allow the priority of an investigation to be set. This must be associated with specific timelines.
- Based on the investigation classification, the system will automatically present the user with a set of recommended jobs to be completed over the course of the investigation. This will be based on a taxonomy of jobs that is set-up in the system by an administrative type user. The user must have the option to create additional jobs if necessary.
- The system will allow a user with the appropriate access privileges to add members to the investigative team and assign these members to a role within the team. The following information is entered in order to add a member to the team:
  - Garda unique personal identifier
  - Civilian unique personal identifier
- The system will allow a user to search for a member they wish to assign to the investigation team. The name and unique personal identifier of the user must be returned and populated into the investigation record.   

- The system will allow a user with the appropriate access privileges to remove a member from the investigative team.
- 

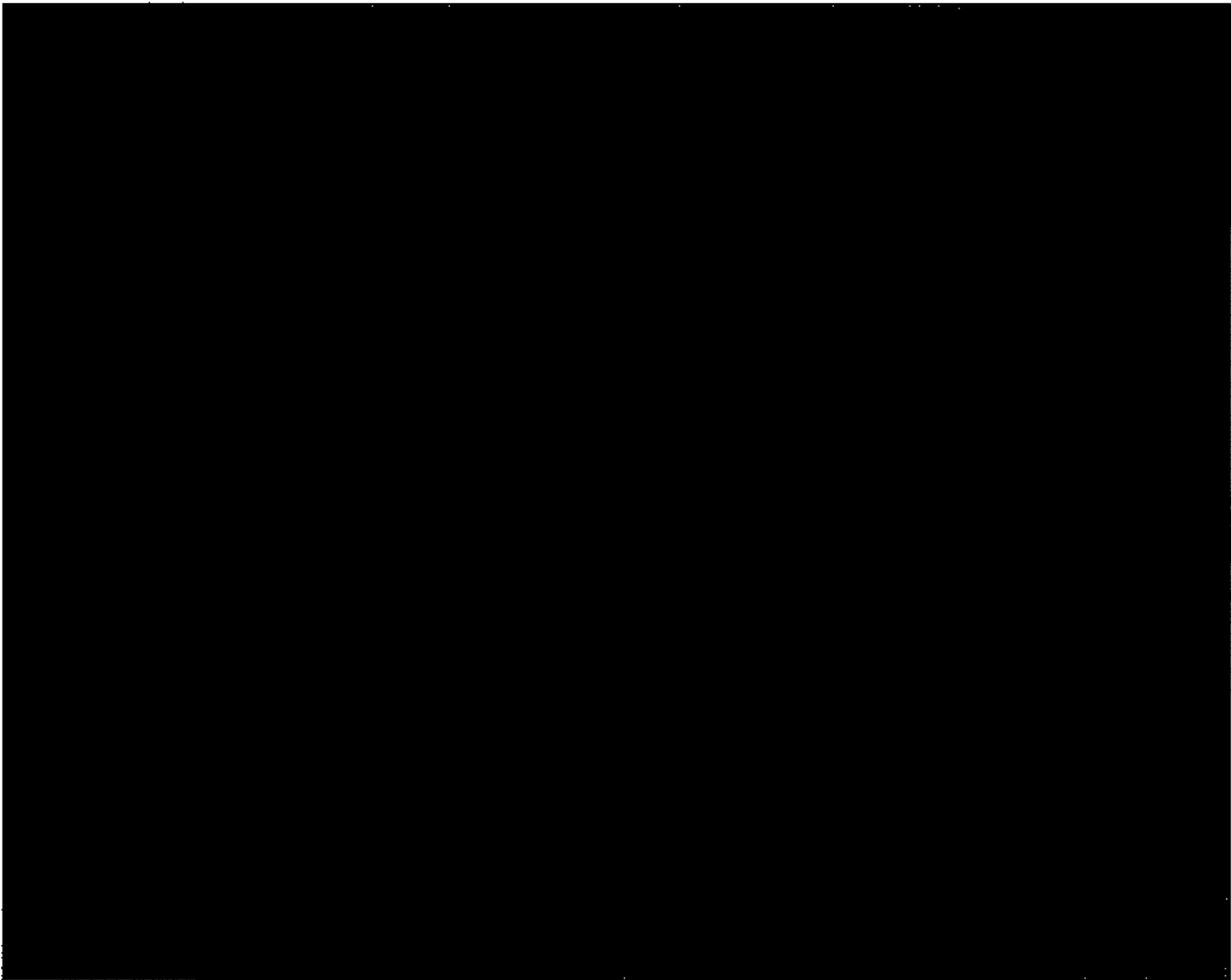
### Jobs

- The system must allow a user to create and update a job. There must be a one to many relationship between the major investigation and job. That is to say, many jobs can be associated with a major investigation.
  - The following information must be stored for a job:

- Job number - Assigned automatically. Consecutive numbers
  - Job category - Jobs must be categorised
  - Assigned to - Details of who the job is assigned to. Many people could work on a job. Details of all the people must be tracked
  - Date and Time Assigned - The data and time the job was assigned to a team member
  - Assigned by - Details of who assigned the job to the team member
  - Contact details - For the person who assigned the job including a phone number and station/location or department
  - Status - The status of the job
  - Due date - The date the job must be completed by
  - Content - Details about the job
  - Result of job - Includes both the result of the job and action taken. Could result in a document being attached.
- The user must also be able to create a new job(s) from within a job record. The link between the two records must be maintained automatically by the system.
  - The system must allow a user to assign a job to a member of the investigative team.
  - The system must allow a user to reassign a job to another member of the investigative team.
  - The system must allow the status of a job to be updated and tracked. The following status values must be incorporated into the system:
    - Pending Document Input - A lengthy document may take some time to enter and some part of it may be entered by an administrative type user (for example, a typist)
    - Pending Review - All documents entered or modified by an administrative type user must be automatically set to this status

- The system must allow a priority to be set for the job which reflects the importance and urgency of the job.
- The system must allow a user to capture the result of a job. This could involve the attachment of a document or object to the job.
- The system must allow a member with the appropriate privileges to capture any comments they have regarding a job.
- The system must automatically maintain a jobs list which allows a user to view and manage the jobs. The user must be able to filter this list as necessary. Specific filters that have been defined to date include the following:
  - Job status
  - Job assigned to
  - Due date
  - The user must be able to print the jobs list.
- A user must be able to see a list of his/her own jobs and filter according to the status of the job.
- The system must allow a user to electronically send a list of jobs to a member of the team. This could simply contain a list of jobs for the specific person or be a list of all jobs.
- The system must allow a user to print the jobs list (sheets).
- The system must allow a user to link jobs to other jobs at the time of entry or at a later date. This will show the chain of jobs within an investigation.
- The system must allow users to search for jobs based on specific structured fields and a free text search.
- The system must allow a user to sign-off particular jobs as complete and enter a comment. Once signed off, job details and document details if attached, must be locked down and must not be editable.

- The system must allow for a job, statement or other document to be flagged as noteworthy or for further discussion at a morning conference or management briefing.
- The system must allow a user to mark a record as sensitive restricting access to these files to specific users within an investigation team.
- The system must allow a user to track exhibits as follows:
  - View a list of all exhibits associated with the major investigation
  - View the chain of custody for an exhibit
  - View the final outputs produced for the exhibit
- The system must provide a threaded graphical display of all the jobs outlining the investigative routes taken.




### Reports

- The system must enable the generation of the 'Bingo Card' report. This report, which is used in morning conferences and management briefings, includes the following information in relation to all jobs:
  - The status of the jobs
  - Details of who the job is assigned to
  - Job summary details
  - Items flagged as noteworthy for discussion.
  - Blank rows for manual input during a conference
- The system must allow for the generation of a report that outlines the status of all jobs.
- The system must allow reports to be generated which list all jobs, statements or other documents that have been marked as noteworthy for discussion at a morning conference or management briefing.
- A number of statistical reports have been defined (note a full list of the reports required will be defined during the detailed design phase):
  - Number of jobs outstanding
  - Number of statements taken
  - Number of statements by type
  - Number of questionnaires by location

### Key Events

- The system must allow a user to create key events which occur during the lifetime of a major investigation. A key event would be created for every major decision or event which takes place, for example the death of a witness,

or a decision by the investigative team to focus on one avenue of investigation over another.

- The user must be able to select a type or category of key event record. Each type of key event record must be linked to a specific set of data fields that must be entered.
- The system must allow a user to enter decision details into a key event. It must be possible to record details relating to the decision made and reasons why the decision was made.
- The user must be able to update a key event.
- The system must display a complete list of the key events associated with the major investigation.
- The system must enable a job to automatically trigger the creation of a key event record. It must be possible to configure some jobs to do this automatically. The system must also allow a user to manually trigger the creation of a key event from a job.
- 
- The system must allow users to mark a key event for discussion at a morning conference.
- The system must allow a user to link a key event to one or more jobs or one or more documents.
- The system must allow a user to generate an executive summary report which summarises the key events over the course of the investigation and the associated dates and times. This will provide a user with a high level view of the status of a case.
- The system must allow a user to generate a report which includes the key events that were flagged for discussion at the conference.

### Preservation of Scene Log

- The system must allow a user to record details relating to the scene of an incident. This would include, for example, a description of the scene, where the scene is located and weather details.
- The user must be able to store details of all visitors to the scene of an incident. This would include, for example, name, date and time scene visited and reason for visit.

### Disclosure Management

- The system must allow the user to create and update a disclosure and record details relating to the disclosure. This includes:
  - Date by which the disclosure must be made
- The system must alert the user to the fact that the deadline for the disclosure is approaching and action must be taken.
- The system must allow the user to search for the appropriate documents and link them to the disclosure. Disclosure details must be recorded against the document.
- The system must allow the user to send the disclosure details to the State solicitor electronically.
- The system must allow the user to record the following details against the disclosure:
  - Date the disclosure was sent
  - To whom it was sent

### Prepare Final Report for DPP

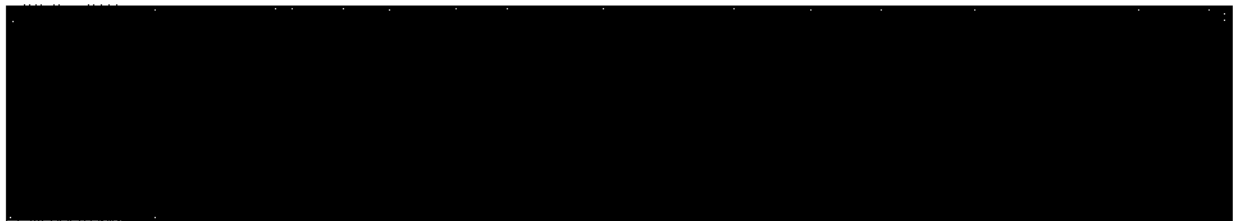
- The system must allow the user to create a final report and record details relating to the final report. The user must subsequently be able to update the final report details.



- The system must allow the user to search for the appropriate documents. The user must be able to enter the reason why the document is being included in the final report or why it is not being included in the final report. These details must be recorded against the document.
- The user must be able to include details of the exhibits in the final report.
- The system must allow the user to send the final report to the interested party electronically.
- The system must allow the user to record the following details against the disclosure:
  - Date the final report was sent to the DPP
  - To whom within the Office of the DPP it was sent

#### General MI Requirements

- The system must include functionality to verify the identity of a person.
- The system must allow for alerts to be set-up in the system and sent electronically to another member or section.
- The system must include register an interest functionality. A user must be able to define their interest in a certain piece of information and be automatically notified of any information added to the system in connection with the interest.
- The system must allow a user to specify keywords in the system. The user must be able to carry out a keyword search whereby only words marked as keywords in the system are searched.
- The system must allow for a record to be marked as inactive in the system according to specific business rules and user access privileges. *This functionality must be provided as a user must not be able to delete a record from the system. Records must be clearly marked as inactive in the system.*





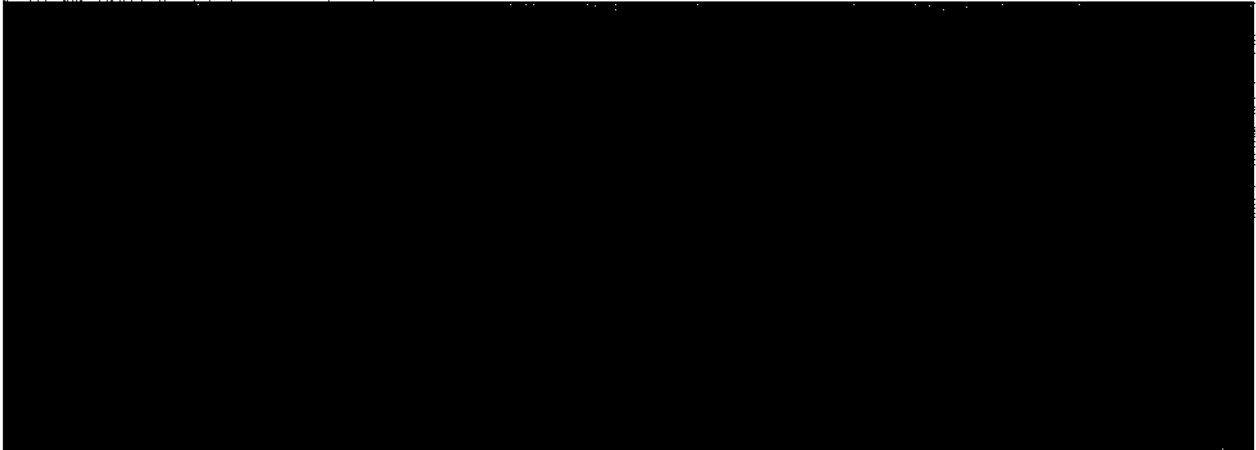
- The system must provide the functionality to escalate an issue when necessary.
- The system must provide the facility for the user to request authorisation to perform a specific action from another member. For example, authorisation may be required to disclose a particular document.
- The system must provide the facility for a member to grant authorisation to another member to perform a specific action.

### Search

- The system must allow a user to perform a simple or advanced search within a Major Investigation file. The exact requirements for each will be defined during the detailed analysis and design phase.
- The system must allow a user to perform a search across linked Major Investigations files.
- The system must allow a user to perform a simple or advanced search across all Major Investigation files. The results returned may be restricted to simply allow a user to determine if there is a "hit" on a person's name. For example, an authorised user may be able to perform a search on John Doe, and may identify that this person's name is in a statement taken in a given investigation without being allowed to view the statement itself. This will be determined during the detailed analysis stage.
- The system must allow the user to specify the content type across which to search, for example statements, questionnaires, interview notes and jobs. This will enable a user to search for a suspect's name across all data associated with the investigation or just within a specific section of the data stored (for example statements).
- The system must allow the user to search for all data, both structured and unstructured. This includes for example, the header and footer data, the document text and audio files. For example, search for all statements

collected by a certain team member, or all documents collected on a specific date.

- The search facilities of the system must be capable of restricting access to data based on:
  - Individual files which are marked as sensitive
  - Individual investigations. Rank and file Garda members must only be able to access data relating to investigations on which they are specified as team members. An authorised user on an investigation team must be able to search across documents on Major Investigations that are linked together.

- 
- Rank: Members above a certain rank must be able to view each investigation to determine the status of the case and the amount of progress made to date.

#### Financial Costing of a Major Investigation

- The system must provide the facility for the user to record the hours spent by each team member on the Major Investigation team. This must be further broken down by type of hours, for example ordinary hours and overtime hours.
- The system must provide the facility for the user to record the travel and subsistence hours spent by each team member on the Major Investigation team. This must be further broken down by number of hours and overnight hours.

- The system must provide the facility for the user to record the unsociable hours spent by each team member on the Major Investigation team. This must be further broken down by type of unsociable hours, for example night duty, Saturday, Sunday, public holiday.
- The system must provide the facility for the user to record the mileage incurred by each team member on the Major Investigation team. This must be further broken down by type of mileage, for example official vehicle and private vehicle.
- The system must provide the facility for the user to record other costs incurred by each team member on the Major Investigation team.
- The system must automatically extract the following from the HRM or Financial Management System as appropriate.
  - Hourly rates
  - Travel and subsistence allowance rates
  - Unsociable allowance rates
  - Mileage allowance rates
  - Other rates if appropriate
- The system must automatically calculate the total costs associated with an investigation. It must be possible to breakdown the total costs incurred by the different categories including hours, mileage, travel and subsistence, unsociable allowances and other costs. It must be possible to further breakdown the costs by each of the categories defined for each, for example the total cost of Travel and Subsistence overnight hours. The system must provide the facility to do this both for an individual member and for the entire investigation and for different periods of times and weeks.
- The system must allow for the generation of the following reports (Additional reports may be identified during detailed design):
  - Weekly report
  - Total costs to date
  - District/section costs to date

### Configurable Solution

- The system must provide functionality for an administrative type user to configure the values in the drop-down lists when necessary.

## 2.1 Proposed Solution

As outlined in Part 3 of Schedule B in the Agreement, the Software deliverables for Phase 3b of the MIMS project include an Investigations Management Component in accordance with the functional requirements set out above.

Following a review of the proposed solution, the use of a Customised Software solution is considered to be the most economically and technically advantageous solution to deliver Phase 3b of the MIMS project. The costs are set out in Section 4 below.

The Customised Software will be owned by An Garda Síochána in accordance with section 7 of the Agreement.

## 2.2 Approach to Work

The overall work effort for Phase 3b will be broken down into work packages and tasks. Work packages comprise of a series of tasks. The key tasks that will be completed for each of the Phase 3b work packages are outlined below.

**Project Management & Planning** - This stage covers the initiation and planning activities required to mobilise the Investigations Management Phase, as well as the ongoing Phase 3b management activities required to ensure that the Phase is delivered. The activities to be performed are as follows:

- Confirm the Phase scope and expectations;
- Manage the Phase scope, resourcing, budget and schedule;
- Manage the quality, issues and risks;
- Manage the Phase finances;

- Administer the Agreement;
- Maintain the Phase work plans;
- Report on the progress of the Phase; and
- Track the Phase deliverables.

**Requirements Analysis** - The purpose of this stage is to review the existing Investigations Management business processes and to review and confirm the functional and technical requirements for the new Investigations Management solution. The key inputs will include:

- The current baseline understanding of the requirements as outlined in the RFT (Request for Tender) documents;
- Requirements gathering workshops with key functional experts to confirm functional requirements;
- Technical architecture requirements workshops taking into account AGS standards for security, resilience, environment configurations, AGS configurations and recommended deployment, operations and service introduction procedures;
- Document the full matrix of Investigations Management functional and technical requirements arising out of the workshops.

**Functional Design & Technical Design** - The purpose of this stage is to produce the design specifications for the system to describe each element of functionality being provided for AGS. This will include:

- Configuration specifications for the installation of the Investigations Management Component Software and database;
- Functional and technical specifications for customisations to screens, menus, reports and interfaces in order to satisfy the requirements;
- Technical specifications for processing logic within the system, deployment of the Customised Software within existing environments and AGS workstations, as well as interfaces with other applications (if appropriate);
- Database design specifications including detailed definitions of entities, attributes and relationships.

These design specifications will be reviewed and agreed, as they form an important basis for the development and configuration.

**Installation, Configuration and Build** - The purpose of this stage is to build technical environments and install the Customised Software for configuration and development of custom components as per the design specifications:

- Build the development, test, training, production and disaster recovery environments and configure for installation of Customised Software;
- Install the Customised Software and database on the development environment;
- Test the Customised Software to ensure basic functionality can be performed without significant error;
- Document any configuration changes required, arising from pipe-clean tests
- Implement functional and technical configuration changes to the Development Environment, based on the agreed functional and technical requirements;
- Development of customisations to the Customised Software as per the specifications produced in the design phases;
- Document final functional and technical configuration settings and build, including:
  - Full suite of detailed instructions and configuration settings for the installation of the Customised Software and database, and for making functional and technical configuration changes to the Customised Software and database;
  - Updated server and environment design specifications;
  - Deployment, operations and service introduction procedures;
  - AGS workstation build and browser settings.

**Testing** - The purpose of this is to test the Investigations Management system for conformance to the design specifications. The activities to be performed as follows:

- Conduct Unit Testing of components for conformance to the specification;
- Conduct Assembly Test to ensure that all components interact correctly without significant error;
- Installation of the Intelligence Management system and database to System Test and Technical Test Environments;

- Complete and agree System Test Approach which includes end-to-end functional testing to ensure that the system behaves as specified, from a business, user and technical perspective. This will also include an approach for functional testing of data migration in line with the Data Migration Approach document;
- Prepare System Test Scripts and data;
- Execution of System Test in accordance with the test approach;
- Document and Implement any changes arising from System Test;
- Complete and agree Technical Test Approach Document, which includes integration, security and performance test plans. This will also include an approach for technical testing of data migration in line with the Data Migration Approach document;
- Preparation of Technical Test Scripts and data;
- Loading of performance test data to the Performance Test / Technical Test Environment;
- Execution of technical testing and resolution of any significant performance issues with the Investigations Management system;
- Document and implement any configuration changes arising from Performance Test;
- Preparation of User Acceptance Testing (UAT) scripts and test data;
- Installation of the Investigations Management system and database to UAT Environment;
- Execution of UAT, and resolution of any significant issues that arise during UAT;
- Document and implement changes arising from UAT;
- Document a revised functional specification for the Investigations Management System;
- Document a revised Investigations Management configuration manual, containing:
  - Full suite of revised functional and technical configuration settings for the installation of the Customised Software and database, and making functional and technical configuration changes to the Customised Software and database;



- Revised Investigations Management server and environment design specifications;
- Revised deployment, operations and service introduction procedures;
- Revised Investigations Management AGS workstation build and browser settings.

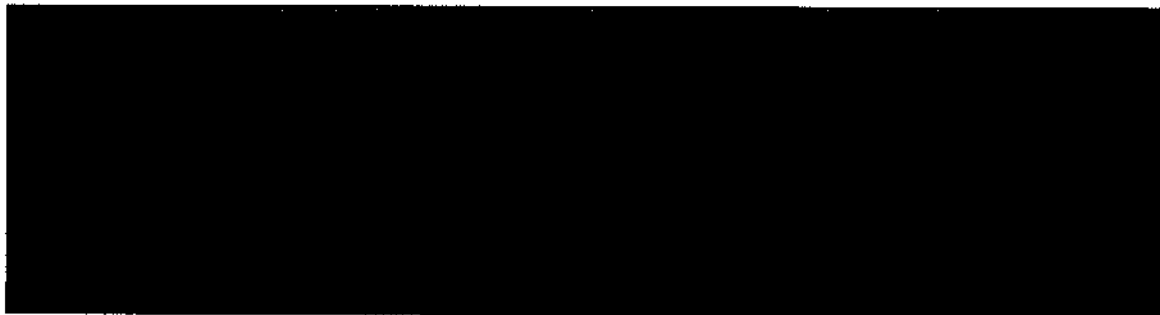
**Business Process Design & User Training** – the activities to be performed are as follows:

- Document business process procedures and flows;
- Complete and agree Training Plan;
- Produce the full suite of training materials;
- Supply training materials to AGS;
- Installation of the Investigations Management system and database to Training Environment.

**Production Installation and Implementation** – the activities to be performed are as follows:

- Complete and agree a deployment plan for the Investigations Management system;
- Deploy the Investigations Management system and database to the production environment;
- Prepare and conduct Operational Readiness Testing (ORT) to ensure that the IT Operations unit can build and operate the Phase 3b solution successfully;
- Copy the configured database to the all pre-live environments;
- Provide post-implementation support.

### 2.3 Security Arrangements





### 3. Project Plan and Control Mechanisms

This section provides details of the individual plan for Phase 3b of the Project. The Project will be delivered using a phased implementation approach. This phased approach will enable new functionality and technology to be developed and delivered in successive phases.

The implementation timeframe for Phase 3b of the Project is summarised in Table 3.1 below. Target completion dates for Phase 3b will be dependent on the Phase 3b start date.

MIMS Phase 3b Milestones	Implementation Timeframe
Phase 3b – Investigations Management	18 months

**Table 3.1: Implementation Timeframes for Phase 3b**

It is proposed that Phase 3b will be deployed on ICT infrastructure to be provided by AGS. As a result of this, the implementation timeframe above is dependent on the availability of the GARDAIS infrastructure and resources to facilitate the integration of Phase 3b System Components when required.

#### 3.1 Project Plan

The high-level implementation plan for Phase 3b – Investigations Management is outlined in Figure 3.1 below. The target duration period for Phase 3b is 18 months after the completion of the initial mobilisation phase expected to last 4 weeks.



**4. Costs**

It has been agreed with AGS that AGS will pay Accenture [REDACTED] to provide Services set out in this PID for the delivery of Phase 3b of the MIMS Project. This excludes any additional costs for both hardware and Software as outlined below.

**4.1 Phase 3b Services Costs**

Based on a review of the functional and technical requirements, services fees for Phase 3b will be [REDACTED] Billable expenses of up to [REDACTED] will be invoiced as incurred for the provision of the Services.

The payment schedule for the services described in this PID is outlined in table 4.1.1 below and is based on the payment terms outlined in Schedule C of the Agreement.

MIMS Phase 3b Payment Schedule for Services		
Milestone	Payment (excl. VAT)	Payment (incl. VAT)
Month 1		
Month 2		
Month 3		
Month 4		
Month 5		
Month 6		
Month 7		
Month 8		
Month 9		
Month 10		
Month 11		
Month 12		
Month 13		
Month 14		
Month 15		
Month 16		
Month 17		
Month 18		
Month 19		
Month 20		
<b>Total Payment Amount</b>		

**Table 4.1.1: Payment Schedule for Fees Due**

Fees shown in table 4.1.1 are illustrated with and without VAT. VAT has been calculated using a VAT rate of 23%. Any changes to the VAT rate will impact the costs of Services including VAT.

All services costs described are inclusive of a discount of 8% as required by Department of Finance Directive 02/09.

#### 4.2 Phase 3b Hardware and Software Costs

The indicative Hardware costs for Phase 3b – Investigations Management are detailed in Table 4.2.1 below. The specification and amount of Hardware may be amended depending on its availability from Hardware vendors and may be substituted with similar Hardware. The AGS will provide the Hardware below via existing infrastructure or through procurement. The AGS may instead at its discretion, if procurement is required, request Accenture in writing to procure such Hardware.

Item	Description	Quantity	Unit Cost	Total Cost
Blade HW	BL460 Gen8	4		
Blade Support	HW Support (3 yr)	4		
Storage	SAN Storage (P7400)	2		
Storage Support	SAN Support (3 yr)	2		
<b>Total (Excl. VAT)</b>				
<b>Total (Incl. VAT)</b>				

Table 4.2.1: Hardware Requirements\*

There will be a requirement for AGS to procure Software licences in relation to the delivery of Phase 3b. In this case Accenture will endeavour to accommodate the most cost effective solution, including the use of Open Source Software where appropriate. The Client will provide the Hardware below via existing infrastructure or through procurement. The Client may instead at its discretion, if procurement is required, request Accenture in writing to procure such Hardware.

The indicative Software requirements for this Phase are detailed in table 4.2.2

Item	Description	Quantity	Unit Cost	Total Cost
Red Hat Linux Server (2 Sckt)	License + 3 year support	8		
VMware SW	vSphere	8		

Total (Excl. VAT)			
Total (Incl. VAT)			

Table 4.2.2: Software Requirements and Associated Costs\*

Item	Description	Quantity	Unit Cost	Total Cost
VMware SW Support	Per annum			
Total (Excl. VAT)	Per annum			
Total (Incl. VAT)	Per annum			

Table 4.2.3: Software Support Costs\*

\* Assuming re-use of existing Blade Chassis, Storage Chassis, Alfresco and Oracle infrastructure in both data centres

The Hardware and Software necessary to host the functionality to be provided by Phase 3b –Investigations Management will be reviewed during the detailed design activities which will be conducted at the start of the Phase.

#### 4.3 Reconciliation of Actual Costs against Estimated Costs

Subject always to the provisions of clause 5 and clause 14 of the Agreement, in the event that the Agreement is terminated for any reason, Accenture will reconcile the actual costs earned in the delivery of Services up to the date of such termination (based on the tables set out in Section 4.1 above and as may be agreed) against the aggregate amounts paid by AGS up to the date of such termination pursuant to Table 4.1.1 above. If the amounts paid by AGS to Accenture up to the date of such termination exceed the actual fees earned by Accenture, Accenture will thereupon refund to AGS any surplus fees which have been paid by AGS within 30 days of the date of such calculation.

If the amounts paid by AGS to Accenture up to the date of such termination is less than the amount fees to which Accenture is entitled under this PID, AGS will thereupon pay to Accenture any shortfall in fees within 30 days of the date of such calculation.

If AGS requests additional work to be undertaken which will result in additional effort not covered by the scope of this PID, this will be agreed with Accenture and documented and any associated additional costs will be invoiced to AGS separately.

This additional effort must be requested by AGS in writing and any associated costs agreed in advance.

## 5. Project Organisation

In accordance with and subject to clause 10 of the Agreement the project organisation structure and steering arrangements are outlined below. It should be noted that the organisation structure will change over time to reflect work in progress.

Figure 5.1 provides a high-level view of how the project is organised for Phase 3b.

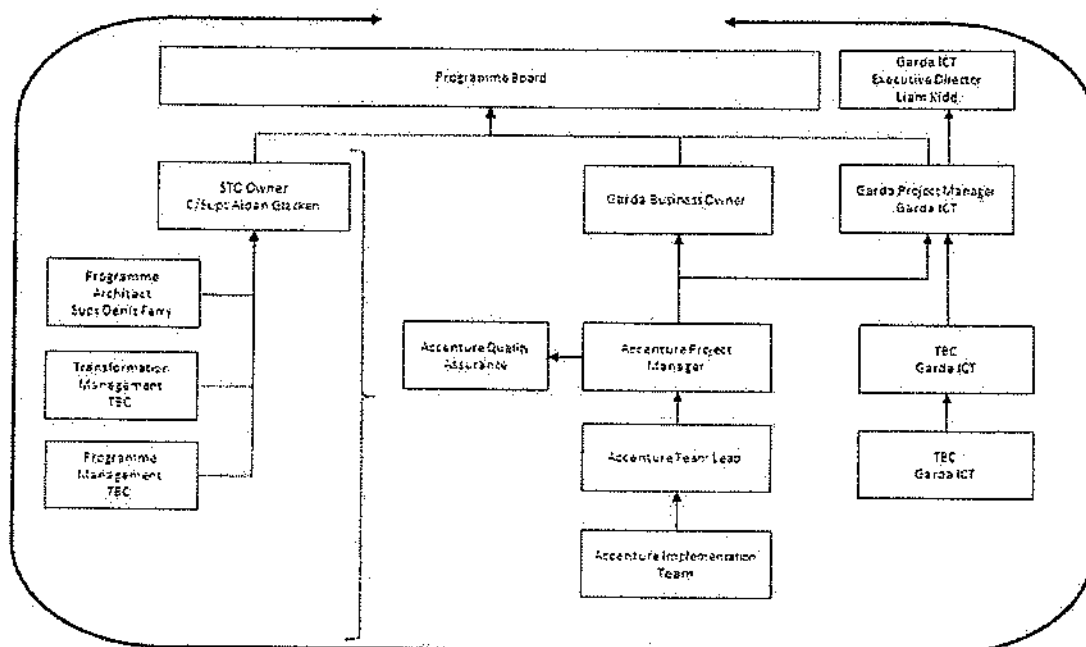


Figure 5.1: Organisational Structure - MIMS Phase 3b

### 5.1 Governance

The Governance model for Phase 3b as per the Garda Transformation Programme is described in detailed below.

#### Programme Board

This section provides details of the responsibilities of the Programme Board. MIMS Phase 3b has been identified as a priority project under An Garda Síochána's Policing & Security with TRUST Transformation Programme and as such will be the

responsibility of one of four newly established Programme Boards. The Programme Board will oversee the planning, design, build, deployment and benefits realisation phase of the Project. The overall responsibility of the Programme Board is to:

- Appoint a Business Owner with responsibility for Project Implementation
- Provide overall guidance and direction to the Project
- Ensure that the Project is conducted to the agreed project management method/standards
- Report on the Project's progress to the senior leadership of the organisation.

At the beginning of each Release, the Programme Board will:

- Ensure that the project complies with the agreed scope and business objectives;
- Approve the project documentation and associated work plans; and
- Authorise and commit resources to the Project.

As the Phase progresses, the main responsibilities of the Programme Board are to:

- Monitor project progress and status against budget and schedule;
- Monitor status of change management, business readiness and training delivery
- Review and approve actions to resolve issues or address exception situations;
- Review and approve impact assessments of change control notices raised sign off PRINCE deliverables;
- Sign off each completed release; and
- Review plans for subsequent Project stages.

At the end of the Phase, the main responsibilities of the Programme Board is to:

- Ensure that all Deliverables are complete and delivered; and
- Authorise Phase closure.

### **Business Owner**

The Business Owner is responsible for the overall delivery of the project and ensuring that the project meets business requirements and delivers the stated benefits for the organisation.



At the outset of the project the business owner is responsible for developing the strategy, business case and high level requirements for the project. The business owners is also responsible for identifying and documenting the benefits to be delivered by the project.

Once the project reaches the implementation phase the Business Owner will review and approve project deliverables and status reports in advance of Programme Board meetings at each phase of the Project.

The Business Owner will also be responsible for escalation of risks and issues to the Programme Board.

Following deployment, the business owner will be responsible for measuring and tracking benefits realisation.

#### **Strategic Transformation Office**

The Strategic Transformation Office (STO) will be responsible for ensuring that the project adheres to the Programme Management and Governance structures throughout the project lifecycle, under the Garda Transformation Programme. The Strategic Transformation Office will provide three key functions to the Transformation Programme.

##### **1. Programme Architecture**

Ensure the overall strategic direction of the Transformation programme is maintained. Support Programme Boards and Business Owners throughout implementation of Transformation projects.

##### **2. Transformation Management**

Provide an overall approach to programme wide communications as well as support for Transformation management and business readiness activities on individual projects.

##### **3. Programme Management**

Track and monitor high level status for each project and report on overall Programme status to Garda leadership. Ensure projects adhere to the defined governance and delivery standards under the Transformation Programme.

Status reports, risk/issue logs and high level project plans will be maintained via the Programme Management Office within the STO.

A representative from the Strategic Transformation Office and An Garda Síochána ICT will sit on the Programme Board, along with the Business Owner, to ensure the project delivers the agreed business objectives and that the overall strategic direction of the Transformation Programme is maintained.

#### **Garda Project Manager**

The Garda Project manager is responsible for oversight of the project delivery team and ensuring that project milestones and deliverables are completed on time and to the required standard during the implementation phases of the project. The Garda Project manager is appointed from within the ICT Section and will be supported by a management team from this section.

#### **Accenture Project Manager**

The primary responsibility of the project manager is to ensure that the Project as a whole produces the required Deliverables to the required standard of quality, and within the specified constraints of time and cost.

The Accenture Project Manager for Phase 3b is accountable to the Business Owner, Garda Project Manager and the Programme Board.

The Project Manager will work with the Garda management team to:

- Plan the Phase and develop the documentation for Phase 3b;
- Agree the objectives and focus for each team; and
- Monitor progress and use of resources, and identify and agree corrective action where necessary.

The Project Manager will work closely with the Project Assurance Team to:

- Facilitate the implementation of the PRINCE Quality process; and

- Address concerns, issues or other requests for information from the Project Assurance Team.

[REDACTED] will perform the Accenture quality assurance role and will work with the Garda Management team to ensure the agreed levels of service are delivered.

## 5.2 Key Assumptions

- (i) All relevant information and access to resources will be given to Accenture to allow for the effective discharge of responsibilities in relation to this PID.
- (ii) The Investigations Management system will be deployed into the GARDAIS domain.
- (iii) The following existing GARDAIS components will be made available and can be re-used in the technical Architecture of MIMS Phase 3b:



- (iv) The Investigations Management system has assumed that AGS will provide the ICT infrastructure in the GARDAIS environments on which to deploy the solution. This includes server infrastructure (blades, associated chassis and server virtualisation Software) and external storage solution (SAN Fabric) with enough capacity to facilitate the integration of Phase 3b into the GARDAIS domain. Any additional Hardware or Software required to host the Customised Software being provided under the scope of services in this PID will be provided by AGS in accordance with the timelines outlined in this PID.

(v) The Investigations Management system has assumed that the GARDAIS [REDACTED] [REDACTED] solution will be available for integration with the Customised Software being provided in accordance with the timelines outlined in this PID.

(vi) Regression testing of other GARDAIS systems [REDACTED] [REDACTED] will be required to ensure no degradation of performance due to the addition of the Customised Software being deployed to the GARDAIS domain. GARDAIS testing environments and resources will be made available to facilitate the integration and testing of Phase 3b System Components in GARDAIS and associated test environments when required. Subject to clause 17 of the Agreement (Force Majeure) any unscheduled or undue delays in the availability of AGS environments or resources may result in additional Charges provided always that the Parties shall endeavour to progress other elements of the Deliverables to mitigate the impact of any unscheduled or undue delay in availability. As external agencies also share the Garda Integration Broker, coordination of testing activities will also be required with these agencies. AGS will be responsible for organising the testing activities with other parties (internal and external) using the Garda Broker.

[REDACTED]

(viii) It is assumed that support will be available from the existing Garda IT and Telecoms teams for the following activities:

- o Execution of testing, regression testing and end-to-end testing. It is assumed that these environments and associated testing equipment will be prioritised

and made available in line with considerations around the overall AGS testing schedule and priorities.

- [REDACTED]
- (ix) All fees shown in Section 4 have been calculated at 23%. Any changes to the VAT rate will impact the costs of Hardware, Software and Services including VAT.

[REDACTED]

[REDACTED] Any Hardware or Software required under the scope of services in this PID will be provided by AGS in accordance with the timelines outlined in this PID.

- (xi) The Investigations Management system has assumed that AGS will provide the 3<sup>rd</sup> party hardware and software to scan documents. Any Hardware or Software required under the scope of services in this PID will be provided by AGS in accordance with the timelines outlined in this PID.

### 5.3 Key Dependencies on An Garda Síochána

- (i) Any AGS resources who will be involved in the delivery of Phase 3b and who may be responsible for post implementation support will be identified at the start of the Phase.
- (ii) The Accenture and Garda resources identified in dependency (i) will be co-located to facilitate the efficient exchange of information between resources and in accordance with the provisions of Schedule G of the Agreement.
- (iii) Relevant AGS resources will be made available to support the project activities outlined in this PID in accordance with the agreed project plan.

- (iv) All Accenture resources will be provided with reasonable adequate accommodation including network connectivity to allow for the effective discharge of their duties.
- (v) Accenture resources will be provided with the correct level of access (including administrator access where appropriate and in accordance with the provisions of Schedule G of the Agreement) to Hardware and Software to allow for effective discharge of their duties.
- (vi) Any updates necessary on the IT service desk AHD system will be made to allow for the effective reporting of status and service performance.
- (vii)
- (viii) Any additional Hardware or Software required to host the Customised Software being provided under the scope of services in this PID will be provided by AGS.

#### **5.4 Exclusions**

- (i) Post-Implementation support service costs are not included in the fees detailed in Section. 5.
- (ii) Developments of enhancements to the Garda Broker and other GARDAIS systems that are required to integrate with the Investigations Management system.
- (iii) Any networking requirements to facilitate the hosting of the solution.
- (iv) Any hardware associated with the solution (servers, storage, mobile devices etc.).

#### **6. Formal Acceptance**

Formal acceptance of Deliverables from a contractual perspective is defined in Schedule D of the Agreement.

## 6.1 Control Mechanisms

The approach set out below refers to the controls and techniques being used during implementation of Phase 3b – Investigations Management.

## 6.2 Progress Reporting

The focus of progress reporting is to ensure that project management has access to timely and accurate information on Project status against budget and schedule. Project Work planning and Progress Reporting procedures have been defined for the project which outline the process for tracking actual effort invested and progress in completing tasks. These procedures include:

- Rolling up weekly team status report to an overall weekly status report;
- Weekly team status meetings; and
- Weekly management meetings.

## 6.3 Change Control

- All requests for Change Control must be carried out in accordance with clause 19 of the Agreement.

## 6.4 Quality

To control the quality of work undertaken and Deliverables completed during this Phase, a series of procedures, standards and templates have been defined by the project team both during phase mobilisation and as an ongoing activity. Deliverable reviews conducted within Phase teams, and reviews conducted as part of the PRINCE quality review process, ensure that the end Deliverables conform to the standards defined. Accenture's quality system has been certified as conforming to ISO 9001.

The quality assurance approach for MIMS is outlined below and is carried out in accordance with and subject to the terms of the Agreement.

- In accordance with the PRINCE Methodology, the Project will follow a quality review process for each phase (from requirements to deployment stages).

- Accenture will work with AGS to produce documents for a Quality Assurance review. The documents that will be part of the Quality Assurance review for this program are described in Section 3.2.
- The AGS Quality Assurance team will be responsible for reviewing these documents to ensure conformance to standards defined. Documents are released to the AGS Quality Assurance team on the quality review due dates, by Accenture.
- The Quality Assurance team's involvement will be in the review of documents produced as part of the Phase lifecycle, on a phase by phase basis.
- The Quality Assurance Team's responsibilities end for a particular phase, when that phase is released into production. The AGS Quality Assurance team will not be required to play a role in the generation of any Deliverable documents.

## 6.5 User Acceptance Testing

During User Acceptance Testing (UAT) the AGS Quality Assurance team may review the UAT scripts and UAT results/reports, delivered by Accenture, to ensure the System Components meet the required standard of quality. The quality assurance review dates will be included in the detailed Phase 3b plan generated at the start of each phase. Testing will be conducted by Accenture and Garda only in accordance with Schedule D and Schedule G of the Agreement.

In addition to the Quality Assurance document reviews, the AGS Quality Assurance team will sit in on Programme Board status meetings, where the program status will be reported on a monthly basis.

The Quality Assurance cycle is as follows:

### Step 1:

Accenture will deliver the document(s) due for Quality Assurance review to the AGS Quality Assurance team on the dates outlined in the detailed Phase 3b plan.



**Step 2:**

The AGS Quality Assurance team will complete their review and send written feedback to Accenture within 10 working days of receiving document(s). If no written feedback is received within 10 working days from date of distribution, the delivered document(s) will be deemed final.

**Step 3:**

Upon receiving Quality Assurance feedback, Accenture will meet with the Quality Assurance team. Accenture will review feedback with the AGS Quality Assurance team and update document(s) with agreed appropriate changes and produce the final version of the document(s). The final document(s) must be completed within 10 working days of receipt of Quality Assurance written feedback.

**Step 4:**

Accenture will liaise with all relevant stakeholders to obtain sign off of the final document(s). Sign off must be completed within 10 working days from when final document(s) are produced. If no feedback is received from relevant stakeholders within 10 working days from date of distribution of document(s), they will be deemed as signed off. Upon sign off, these document(s) will be distributed to AGS Quality Assurance team and all stakeholders.

## 7. Risk Management

A risk log will be created during the mobilisation phase of the project and this risk log will be maintained by the Accenture Project Manager throughout duration of the implementation.

Risks will be discussed at the weekly project status meeting with the Garda business owner.

The risk log will categorise each risk in terms of the likelihood of its occurrence and the severity of its consequence.

This process will allow the Project Team to:

- Identify the major obstacles (risks) to achieving the Phase 3b objectives
- Identify specific actions which will reduce the risk
- Identify the timescales for evaluating the success or failure of those actions
- Encourage systematic analysis of options for reducing risk.

The key project risks, as agreed with the Garda business owner, will be discussed at the Programme Board meetings.

I agree with the within Project Initiation Document for the purposes of the Agreement and the Notification to Activate Phase



Accenture Project Manager  
For and on behalf of Accenture

Date: 16-12-2015





**AMENDMENT TO THE  
IT SUPPORT AND MAINTENANCE SERVICES AGREEMENT ("AMENDMENT")**

THIS AMENDMENT is made on the 12<sup>th</sup> day of December, 2016

BETWEEN the MINISTER FOR JUSTICE AND EQUALITY of 94 St. Stephen's Green, Dublin 2 and THE COMMISSIONER OF AN GARDA SÍOCHÁNA of Phoenix Park, Dublin (hereinafter "the Client"); and

ACCENTURE a private company incorporated in Ireland with unlimited liability (having a share capital) (Company Number 340745) having its registered offices at 1 Grand Canal Square, Grand Canal Harbour, Dublin 2 (hereinafter "Accenture"),

1. The Client entered into an agreement with Accenture dated 17 November 2006 for the replacement of the Garda Technical Bureau's (GTB) Automated Fingerprint Identification System, the development and implementation of an integration hub and the integration of additional agencies and systems ("the IT Services Agreement").
2. The Client further entered into an IT Maintenance and Support Services Agreement with Accenture dated 22<sup>nd</sup> December 2008 to provide maintenance and support services in respect of all Phases of the performance and delivery of the Services under the IT Services Agreement for a period up to 31 December 2010 ("the Agreement").
3. The term of the Agreement was subsequently extended to 31 December 2016.
4. Prior to the expiry of the Agreement the parties agreed to further extend the Agreement until 31 December, 2019 and works have been carried out pursuant thereto. This Amendment confirms the extension of the Agreement and provides for certain changes to the Services and the pricing arrangements under the Agreement.

NOW IT IS HEREBY AGREED that, in consideration of the mutual covenants, conditions, agreements and payments hereinafter set forth and provided for, the parties hereto respectively covenant with each other as follows:

All capitalised terms used in this Amendment shall have the meaning set out in the Agreement unless provided otherwise expressly or by necessary implication. All references in the Agreement to "Motorola", "Motorola Limited", "Morpho" or "Morpho Trak" shall be replaced by a reference to "Safran Identity & Security".

1. The term of the Agreement is, as and from 31 December, 2016 extended for the period to 31 December 2019 inclusive ("Term") and all related references shall be construed accordingly.
2. The Charges for the Services to be provided during the Term shall be the sum of [REDACTED] along with such other charges for optional additional Services as are set

out at Schedule D to this Amendment and payable under and in accordance with Clause 5 of the Agreement.

3. Section 4.2.3 of the Agreement be and hereby is replaced with the following:

4.2.3 to use all reasonable endeavours to procure all necessary consents for Accenture and Safran Identity & Security to be granted such access to the software and hardware systems and solutions of the Client and such other systems as are described in the Client's RFI ("Client's IT and Network Environment") and that Accenture considers are necessary for the purposes of this Agreement, in particular the provision of remote access to such of the Client's systems and in such manner as is necessary to enable Accenture to provide the Services set out in Schedule A; Accenture shall enter into, and shall procure that Safran Identity & Security enters into, such confidentiality agreements, as may be required for the purposes of such access. Subject thereto and upon reasonable notice in writing the Client undertakes as soon as is practicable to ensure that Accenture and Safran Identity & Security are granted such identified access to and are accorded such reasonable assistance as is required by Accenture and Safran Identity & Security to use such identified software and hardware systems and solutions for the purposes of this Agreement.

4. The following language shall be inserted to become Section 12.5 of the Agreement:

12.5 As at the date of the 2016 Amendment the AFIS system is over ten years old, and whilst still fully operational and functional, it contains a large number of End of Life components. End of Life Components means infrastructure and software that is no longer supported by the third party supplier of such infrastructure or software. Over the term of the proposed maintenance extension, Accenture wishes to formally confirm to the Client that whilst entering into a multi-year maintenance extension (to ensure that the AFIS system remains formally supported), there is an increasing risk to the potential down time that could occur with the failure of one or more of these End of Life Components. Based on this uptime and response SLAs cannot be guaranteed.

5. Section 13 of the Agreement be and hereby is replaced with the following:

13.1 Chief Superintendent IT Operations will have the duty of acting as the Client Contact with Accenture for purposes connected with the Services provided hereunder as of the date hereof.

13.2 [REDACTED] will have the duty of acting as the Accenture Contact with the Client for purposes connected with the Services provided hereunder as of the date hereof.

6. Schedule A of the Agreement be and hereby is replaced with the following:

a) The section entitled "Summary of Accenture Service Hours" be and hereby is replaced by the following:

The Accenture support team will manage all incidents on a 24hour x 7day basis once raised by the users through the An Garda Síochána Service Desk and upon notification of the Accenture AFIS support team by the An Garda Síochána Service Desk.

Accenture will provide the following support:

- On-Site Support: Accenture will provide on-site support in Garda Headquarters between the hours of 09:00 and 17:30, Monday to Friday. Support may also involve remote access by approved subcontractor personnel during this period.
- Out of Hours (OOH) Support: Out of hours support will be provided between the hours of 17:30:01 and 08:59:59 Monday to Friday and 24 hours per day on weekends and Bank Holidays. Out of hours support is provided for Severity 1 and Severity 2 incidents only and will be on an on-call basis via the 24x7 Live Support Team and via remote access by approved Subcontractor personnel.
- Support Personnel - Subcontractor will provide scheduled technical on-site support two weeks per quarter – not to exceed eight weeks (320 hours) per year and not to exceed three (3) weeks per trip.

b) The section entitled "Accenture AFIS Support Team Definition" be and hereby is replaced by the following section:

<b>Description &amp; Accenture Responsibilities</b>
Accenture will provide support services for the AFIS application in the following manner
<ul style="list-style-type: none"><li>• Severity 1 and Severity 2 incidents: on-site support and remote access support inside business hours; on-call support via the 24x7 Live Support Team and remote access support out of hours</li><li>• Severity 3, Severity 4 and Severity 5 incidents: on-site support and remote access support inside business hours only</li></ul>
<b>Timescales</b>
This service support (and the items within it) will be valid from 1st January 2017 until such times as the support and maintenance contract between both parties expires.
<b>Accenture Responsibilities</b>
Accenture is to:



- Provide on-site support during the defined daily working hours. The Support Team is to be onsite during this time unless approval has been granted by An Garda Síochána in relation to other arrangements and may include remote access support by approved subcontractor personnel.
- Provide out of hours support to AFIS users managing incidents with logging, classification, tracking and resolution as defined by the An Garda Síochána Service Desk and including:
  - On-call support via the 24x7 Live Support Team and may include remote access support by approved subcontractor personnel.
  - Escalation to support groups within Accenture and to agreed third parties, for all incidents
- Provide environment support across primary and DR server rooms for:
  - Production
  - Pre-Production
  - Test and Development Environment (TED)
  - Application Management
  - Training Environment
- Operationally Manage vendors including:
 
  - Any other Accenture sub-contractor
- Provide Application Support for:
  - Infrastructure management tools implemented by Safran Identity & Security (HP Openview)
  - AFIS BIS Application
  - Provide Oracle DBA support service for Safran Identity & Security/AFIS related databases
- AFIS Support Team or 24x7 Live Support Team to contact Safran Identity & Security/sub-contractor Customer Support Center (CSC) to log an incident/ service request call. Calls will be logged via the following methods:
  - Dedicated International Customer Hotline
  - eMail Support Request
  - Virtual Incident Processing (VIP)

Once logged all service request calls will be tracked through to resolution.

- Provide Service Level management including:
  - Agreed service reporting:
    - Monthly Service Performance Report (SPR) for all calls raised with customer support centre
    - Weekly Standard Period Report detailing issue raised and closed within that week
    - Provide quarterly availability report of the AFIS system
  - Agreed service reviews
  - Agree to work towards Continuous Improvement initiatives in collaboration with An Garda Síochána.
- Provide AFIS application support including installation and maintenance of any related software and hardware together with third party management for any vendors that form part of the Safran Identity & Security AFIS application. Responsibilities include:
  - Responsible for installation, functional test, technical test and issue resolution
  - Provide weekly update on all open software issues
  - Co-ordination of any rework in relation to fixing issues
  - Documentation of the implementation
- Client acknowledges and agrees that the current AFIS System in place in An Garda Síochána contains a number of End of Life Components. Issues and/or outages related to the system may be delayed based on these components. Subject to this, Accenture will provide resources for all process services and interactions as described in Section 3 and detailed later in this document.

c) Section 3.4 entitled "AFIS -- Service Item 4: Service Support and Management" be and hereby is replaced by the following section:

Item Description
The support provided by Accenture and the hours during which the service will be supplied.
Indicative Service Levels
<p><b>Support Hours</b></p> <p>Core support business hours are: 09:00:00 to 17:30:00 Monday to Friday</p> <ul style="list-style-type: none"> <li>• On Site Support: Accenture will provide on-site support in Garda Headquarters between the hours of 09:00 and 17:30, Monday to Friday. Support may also involve remote access by approved subcontractor personnel during this period.</li> <li>• Out of Hours (OOH) Support: Out of hours support will be provided between the hours of 17:30:01 and 08:59:59 Monday to Friday and 24 hours per day on weekends and Bank Holidays. Out of hours support is provided for Severity 1 and Severity 2 incidents only and will be on an</li> </ul>

<p>on-call basis via the 24x7 Live Support Team and via remote access by approved Subcontractor personnel.</p> <ul style="list-style-type: none"> <li>• Support Personnel – Subcontractor will provide scheduled technical on-site support two weeks per quarter – not to exceed eight weeks (320 hours) per year and not to exceed three (3) weeks per trip.</li> </ul>
<p><b>Accenture Responsibilities</b></p> <p>Make use of An Garda Síochána Incident Management Tool to ensure that there is smooth handover of Incidents, Problems and Changes to third parties and Accenture</p> <ul style="list-style-type: none"> <li>• Provide support during agreed hours</li> <li>• Ensure that Production Data is not accessed or amended by Accenture or any third party personnel</li> <li>• Ensure appropriate resources are available to support service and incidents that are escalated appropriately</li> <li>• Provide an escalation Point of Contact to An Garda Síochána</li> <li>• Ensure all third parties have required security clearance for onsite work and have appropriate authorisation for remote access</li> <li>• Report all Severity Incidents to An Garda Síochána</li> </ul>
<p><b>An Garda Síochána Responsibilities</b></p> <ul style="list-style-type: none"> <li>– Provide an escalation point of contact to Accenture</li> <li>– Inform Accenture of any incident that may impact on Accenture's provision of service.</li> </ul>
<p><b>Other Points to Note</b></p> <p>None</p>
<p><b>Method of Measurement</b></p> <p>None</p>

d) Section 3.4.1 entitled, "AFIS – Service Item 4a: Incident Management" is replaced with the following

Item Description
<p>Client acknowledges and agrees the AFIS System contains a number of End of Life Components which are outside the scope of this Agreement. The Client is currently working with Accenture to discuss the changes to be implemented in order to address issues with End of Life Components, which will be separate from the scope of services and charges set out in this Amendment and will be the subject of one or more separate</p>

**Change Control Notes.** Client acknowledges and agrees Accenture is hereby excused from failure or delay in meeting the response times outlined in table Severity Level Response Time Table set out below. Both parties now agree this table is an "Indicative" Severity Level Response Time Table and Accenture will not be liable under the Agreement to Client whatsoever for any failure or delay on its part in meeting the response times outlined in table Severity Level Response Time Table.

The Incident Management defines the activities required by the Accenture resolving groups to resolve incidents by restoring normal service levels with minimal impact on end users. Incidents are raised by entities contacting the Garda Service Desk. Incident records are classified by category, type and item; and a severity is set on a scale from 1-5. Thereafter the Service Desk will contact and assign incidents to the AFIS Support team during business hours or the 24x7 Live Support Team during out of hours who will contact any third parties as required. The AFIS Support team acknowledges the incident after identifying the fix. Once work starts the status changes to 'Work in Progress' and is then set to 'Resolved' when action is completed. The incident is transferred back to the Service Desk who will close the incident after acknowledgement from the user that the incident is resolved.

Resolution of an incident requires restoration of service, and, where a temporary solution has been applied, identification of a permanent fix with an agreed implementation date. Incidents that require a permanent fix are linked to the problem record for the fix and closed when service has been restored.

- To ensure the best use of resources to support the AFIS Application
- To develop and maintain meaningful records relating to incidents
- To devise and apply a consistent approach to all incidents reported
- To ensure all incidents are resolved as quickly as possible

See Appendix A for Incident Management Flow Diagram

**Service Levels**

**Indicative Severity Level Response Time Table**

Severity Level	Definition	Example	Response Time	Assignment of Incident	Update Time (formal status updates every Y minutes, hours or days)	Escalation Time (formal contact at management level Z minutes, hours or days after incident is passed through)
1	Significant	Loss of	30 minutes	30 minutes	First update	1 hour

	adverse impact on large number of end users OR Result in any material loss or corruption of An Garda Síochána Data	power to production server room causing failure of services, i.e. Total System Failure			60 minutes after acknowledgment of call and every 60 minutes thereafter or as agreed with involved parties	
2	Significant adverse impact on small or moderate number of end users OR Moderate adverse impact on large number of end users	Corruption of any standing data tables e.g. AFIS related code tables; i.e. Critical System Failure	60 minutes	60 minutes	First update 120 minutes after acknowledgment of call and every 90 minutes thereafter or as agreed with involved parties	2 hours*  * N.B. If a Sev 2 is not resolved after 24 hours, then it becomes a Sev 1s
3	Moderate adverse impact on small or moderate number of end users OR Minor adverse impact on large number of end users	One workstation affected preventing it being used for normal operation.	60 minutes	120 minutes	1 day	1 business day or as part of next scheduled maintenance release.
4	Minor adverse impact on small or moderate number of end users	Front end validation not working for optional fields.	240 minutes	TBC	TBC	As part of scheduled maintenance release.
5	Customer request for enhancement to System functionality	None provided	N/A	N/A	N/A	As part of scheduled maintenance release

						Definitions
<p>Accenture Severity 2 will automatically upgrade to a Severity 1 once 24 hours have elapsed on the SLA.</p> <p>If an incident has to be reopened within 2 hours of the original resolution then the SLA will continue as if it never stopped.</p> <p>Accenture should recognise that Severity 3 incidents have the potential to escalate should the service further deteriorate – e.g. one disc failure is followed by another whilst the first remains unresolved. For the benefit of doubt Service Availability means availability of the service as designed and built. If an element of the service for which Accenture is responsible is designed to be resilient, Accenture must undertake all reasonable endeavours to rebuild resilience as quickly as possible.</p> <p>All Severity 1 and 2 incidents should be checked with the user verbally to confirm resolution. For Severity 3 and 4 incidents, resolution details can be mailed to the user who have 72 hours to respond before the incident is closed</p>						
<b>Accenture Responsibilities</b>						
<ul style="list-style-type: none"> <li>• Subject to the relief event language set out in the "Item Description Section" above Accenture will use reasonable endeavours to meet response times set out above in the Indicative Severity Level Response Time Table</li> <li>• Follow the Incident Management process as defined by An Garda Síochána, including Major Incident Process.</li> <li>• Escalate Severity 1 and 2 incidents by phone to An Garda Síochána</li> <li>• Capture and triage incidents to resolver groups for Safran Identity &amp; Security Customer Service Desk</li> <li>• Act as resolver group for incidents for which Accenture has responsibility</li> </ul>						
<b>An Garda Síochána Responsibilities</b>						
<ul style="list-style-type: none"> <li>• When assigning an incident with Accenture, provide a full description including business impact and severity.</li> <li>• Confirm closure of incident, i.e. that issue has been fixed</li> <li>• The Client has sole responsibility for (a) informing Accenture personnel of the requirements of the Client's health and safety policy, and (b) ensuring that any part of the Client's premises used or accessed by Accenture personnel complies with the Safety, Health and Welfare at Work Act 2005 and the Safety, Health and Welfare at Work (General Application) Regulations 2007, in each case as amended, consolidated, replaced or re-enacted.</li> </ul>						
<b>Other Points to Note</b>						
<p>The Client will need to implement an upgrade strategy in conjunction with Accenture to upgrade the End of Life Components to mitigate the service availability and security risks to the AFIS system. This will include, but not be limited to the upgrade of all XP components, the AFIS Matching Subsystem and other End of Life</p>						

**Components:** The effort and costs associated with these upgrades are not covered under this Amendment and will be outlined in detail in the related Change Control Note for each upgrade.

- The response times above are contingent upon the Client providing remote system access for the Accenture Support team and its Subcontractor.

e) The section entitled "Escalation Procedure Time Frame" be and hereby is replaced with the following:

See Section 3.4.1 Service Item 4a: Incident Management for further information

An Garda Síochána shall be entitled to require the attendance of any such person(s) at a meeting with An Garda Síochána and/or such third parties as An Garda Síochána may require to attend, to discuss Service Failure and the steps that are being taken by Safran Identity & Security and Accenture to resolve them. Any such meeting shall be at a time and location that An Garda Síochána shall reasonably require.

Role	Responsibility
Safran Identity & Security Regional Service Manager of EMEA	
Senior Program Manager	

*Table 0-1: Key Safran Identity & Security Representatives*

Role	Responsibility
AFIS Support Team Lead	
AFIS Support Business and Service Delivery Lead	
Accenture Account Manager	

*Table 0-2: Key Accenture Representatives*



7. Schedule B be and hereby is replaced with the following:

**SCHEDULE B  
CHARGES**

The Charges shall be comprised and discharged as set out at Schedule C to the IT Services Agreement. The Charges shall be invoiced on an annual basis.

	2017	2018	2019	Total
AFIS Support and Maintenance Renewal				
I. Hardware & Software Maintenance Costs				
AFIS software & hardware support				
II. Support Services				
AFIS Support Services				
Sub-Total				
Sub-Total				
<b>Total Cost (incl. VAT)</b>				

8. Schedule C be and hereby is replaced with the following:

**SCHEDULE C**

**PAYMENT SCHEDULE**

Payment Schedule	Milestone Payments	
	Expected Date	Value
Hardware & Software Maintenance Costs - 2017	28/01/2017	
Hardware & Software Maintenance Costs - 2018	28/01/2018	
Hardware & Software Maintenance Costs - 2019	28/01/2019	
<b>Sub-Total</b>		
Support Services Q1 2017	30/01/2017	
Support Services Q2 2017	30/04/2017	
Support Services Q3 2017	30/07/2017	
Support Services Q4 2017	30/10/2017	
Support Services Q1 2018	30/01/2018	
Support Services Q2 2018	30/04/2018	
Support Services Q3 2018	30/07/2018	
Support Services Q4 2018	30/10/2018	
Support Services Q1 2019	30/01/2019	
Support Services Q2 2019	30/04/2019	
Support Services Q3 2019	30/07/2019	
Support Services Q1 2020	30/10/2019	
<b>Sub-Total</b>		
<b>Total excl VAT</b>		

IN WITNESS of which this Agreement has been signed by duly authorised representatives on behalf of the parties on the day and year first stated above.

SIGNED by

*x Mirza Amir*

being an Officer so authorised  
by the **MINISTER FOR JUSTICE  
AND EQUALITY** under Section 15(4)  
of the **Ministers and Secretaries  
Act, 1974:**

in the presence of:



Witness

SIGNED by the COMMISSIONER OF  
AN GARDA SÍOCHÁNA  
in the presence of:

*Riamh Keadar*

*[Signature]*

Witness

**SIGNED by**  
for and on behalf of ACCENTURE  
in the presence of:



22/07/2017

*Witness*



T- 61/05<sup>1</sup>



Full file

AN GARDÁ SÍOCHÁNA

---

**IMPLEMENTATION AND INTEGRATION OF THE  
NATIONAL FINGERPRINT IDENTIFICATION SYSTEM**

**FOR**

**AN GARDÁ SÍOCHÁNA,**

**THE DEPARTMENT OF JUSTICE, EQUALITY AND LAW  
REFORM**

**AND**

**THE OFFICE OF REFUGEE APPLICATIONS  
COMMISSIONER (ORAC)**

**INVITATION TO TENDER**

**SECTION A: ADMINISTRATIVE INSTRUCTIONS**

---

**Date: 07/03/2005**



## TABLE OF CONTENTS

<b>1</b>	<b>DOCUMENT PURPOSE</b> .....	<b>3</b>
1.1	PURPOSE & SCOPE OF ITT .....	3
<b>2</b>	<b>ORGANISATION BACKGROUND</b> .....	<b>4</b>
2.1	ORGANISATION BACKGROUND .....	4
<b>3</b>	<b>ADDITIONAL INFORMATION</b> .....	<b>6</b>
3.1	TENDER COMMUNICATIONS .....	6
3.2	WITHDRAWAL FROM TENDER PROCESS .....	6
3.3	OFFER PERIOD .....	6
3.4	NO OBLIGATION TO AWARD .....	6
3.5	PROJECT AND CONTRACT PHASES .....	6
3.6	PLACES OF DELIVERY .....	6
<b>4</b>	<b>SUBMISSION OF TENDERS</b> .....	<b>9</b>
4.1	HOW TO SUBMIT TENDER OFFERS .....	9
<b>5</b>	<b>LAYOUT AND CONTENT OF RESPONSES</b> .....	<b>10</b>
<b>6</b>	<b>EVALUATION OF TENDERS &amp; AWARD CRITERIA</b> .....	<b>14</b>
6.1	EVALUATION PROCESS .....	14
<b>7</b>	<b>CONDITIONS OF TENDER</b> .....	<b>15</b>
<b>8</b>	<b>CONTRACTUAL MATTERS</b> .....	<b>17</b>
<b>9</b>	<b>APPENDIX A - SCHEDULE OF COSTS</b> .....	<b>18</b>
<b>10</b>	<b>APPENDIX B - DECLARATION ON CONFIDENTIALITY</b> .....	<b>19</b>





## 1 DOCUMENT PURPOSE

The purpose of this invitation to tender (ITT) is to seek tender submissions from those candidates invited to participate in the competition being run by the Department of Justice Equality and Law Reform and An Garda Síochána for a new National (Automated) Fingerprint Identification System (AFIS).

This document sets out the administrative instructions for tenders in relation to how they should respond to the tender.

This competition is being conducted under the "restricted procedure" rules governing public procurement in operation within EU member states. The award of contract involves two competitive stages. This is the **second stage**, which constitutes a tender competition confined to the parties pre-selected from the first stage, to whom this ITT has been issued. The requirements set out in these tender documents supersede the information supplied in the pre-qualification documents and the associated questions and answers from the **first stage**.

The awarding authority for the contract is the Department of Justice, Equality and Law Reform and, this tender is being undertaken by An Garda Síochána. The awarding authority reserves the right not to award a contract.

### 1.1 PURPOSE & SCOPE OF ITT

It is envisaged that the contract between the successful supplier(s) (hereinafter referred to as "the supplier") and Department of Justice, Equality and Law Reform on behalf of An Garda Síochána will be fixed-price and consist of the following core requirements:

- Supply, implementation and support of hardware, including storage technology.
- Licensing of appropriate software, including application and database software, for the new AFIS.
- System and database design, development and testing services.
- Implementation services leading to the successful commissioning of the new AFIS (including data and back record conversion).
- Systems Integration Services leading to the successful integration and commissioning of the new AFIS.
- Training Services.
- Post-implementation support services for the overall solution (both hardware and software).

A prime contractor, pre-qualified from the previous stage of this procurement, must host the tender. The awarding authority seeks to award a single contract, to a single primary supplier, for the procurement of all goods and services associated with this supply. The primary supplier will be the single responsible point of contact for the contract delivery.

Suppliers are required to bid for all aspects of this contract. Tenders addressing only part of the requirement will not be considered.

An Garda Síochána will be free to consider and assess variant tender options, which meet its requirements.

It is envisaged that the support and maintenance contract will continue in operation for up to 3 years from final phase of project delivery going live, with a contract renewal review being carried out by An Garda Síochána on an annual basis.

Details of the required services and deliverables to be provided by the successful supplier can be found in **Section B: Requirements Specification**.



## 2 ORGANISATION BACKGROUND

This section provides background to the relevant organisations mentioned throughout this ITT.

### 2.1 ORGANISATION BACKGROUND

#### *The Office of the Refugee Applications Commissioner*

The Office of the Refugee Applications Commissioner (ORAC) is the first instance decision-making body in the Irish asylum system. The office was established under the Refugee Act, 1996 (as amended). Under the Act, the Commissioner is required to investigate each asylum application lodged within the state and to make recommendations to the Minister for Justice, Equality and Law Reform. The Commissioner is also responsible for investigating applications by refugees to allow family members to enter and reside in the State and for providing a report to the Minister on such applications. The Commissioner is independent in the exercise of his or her functions.

For more information see:

<http://www.justice.ie>, <http://www.orac.ie>.

#### *An Garda Síochána*

In terms of organisational structure the Garda Information Technology Division, the Garda National Immigration Bureau (GNIB) and the Garda Technical Information Bureau (GTB) are all divisions of the Irish Police force (An Garda Síochána) under the overall control of the Garda Commissioner.

#### *The Garda Technical Bureau*

The Garda Technical Bureau is the longest established Specialist unit in An Garda Síochána. The Bureau comprises of 9 Sections, each providing a specialist service to An Garda Síochána. They are as follows:

- Fingerprints.
- Ballistics.
- Photography.
- Mapping.
- Document Examination and Handwriting.
- Fogra Tora (Garda information booklet).
- Forensic Liaison Office.
- GCRO, (Garda Criminal Records Office).
- Administration.

Within the various specialist sections, sub-sections have been established. They include:

- Photographic Digital Imaging.
- Shoe mark and Tool Mark Identification.
- Fingerprint Chemical Development Unit.
- Ear prints.
- PRO-FIT (Facial Identification).



- Cheque Fraud.
- Serious Crime.
- Ballistics Data Reference Centre.

The Technical Bureau is headed by a Chief Superintendent (assisted by a Superintendent) who has responsibility for overall management of the Bureau, which has a personnel strength of approximately 200 Garda and civilian staff. The Chief Superintendent reports in turn to the Assistant Commissioner, National Support Services.

#### *The Garda National Immigration Bureau*

The Garda National Immigration Bureau (GNIB) came into operation in May 2000 and is responsible for all Garda operations pertaining to immigration matters in the State. A Detective Chief Superintendent with a Garda staff of 2 Superintendents, 3 Inspectors, 8 Sergeants and 55 Garda heads the GNIB. In addition, there are approximately 34 civilian support staff.

The Bureau became a necessity due to the exceptional increases in persons registering with the former Immigration and Registration Office and associated workload.

#### *The Garda Information Technology Division*

The Garda Information Technology Division is responsible for providing and maintaining leading I.T. support systems serving operational and specialist units within the Garda. A team of approximately 115 Garda and civilian staff, divided into 6 core teams, provides the following key capabilities:

- IT Security and Operations - Provides a 24 hour Service Desk; support services; hardware procurement; rollout of equipment, IT Security; investigation assistance.
- Research and Development - Research requests for new computer systems and technologies and ensure that the technologies chosen are the best and most appropriate solution to meet requirements of specialist sections.
- Project Co-ordination Office (PCO) - Deals with the co-ordination and project management between all the constituencies involved in the major projects, including IT, Telecommunications, Training College, external consultant's etc.
- Project Management Office (PMO) - Provides services to the various project teams, such as document libraries; storage of key documents and deliverables, etc.
- PULSE (Police Using Leading Systems Effectively) Project Teams - Responsible for the design, build and implementation of the PULSE system. PULSE is the largest IT system undertaken by An Garda Síochána and is one of the leading such police projects worldwide. Phase 1 of PULSE was deployed in 1999 and ensures accurate up-to-date information is available to all members in responding to the demands of a modern police force.



### 3 ADDITIONAL INFORMATION

#### 3.1 TENDER COMMUNICATIONS

All communications for this tender must be from the pre-qualified prime contractor only. Additionally, all communication must be in writing and directed to the specified point of contact only.

#### 3.2 WITHDRAWAL FROM TENDER PROCESS

Suppliers are required to advise Eamonn Murray ( [Eamonn.Murray@garda.ie](mailto:Eamonn.Murray@garda.ie) ), immediately, if at any stage they decide to withdraw from the bidding process for this contract.

#### 3.3 OFFER PERIOD

All offers for the contract must be kept open for at least 9 calendar months from the closing date for receipt of tenders.

Suppliers should confirm this in their response(s).

#### 3.4 NO OBLIGATION TO AWARD

Fulfilment of conditions for adjudication or call for tender procedures will not involve An Garda Síochána in any obligation to award the contract.

An Garda Síochána will not be liable for any compensation with respect to suppliers whose tender offers have not been accepted, nor will it be so liable in the event of its deciding not to award the contract.

#### 3.5 PROJECT AND CONTRACT PHASES

The awarding authority seeks to award a single contract, to a single primary supplier, for the procurement of all goods and services associated with this supply. The project itself is expected to be delivered in defined separate phases as set out in Chapter 13 of Section B: Requirements Specification.

#### 3.6 PLACES OF DELIVERY

##### 3.6.1 AFIS

The AFIS will be located in Garda Headquarters (HQ) in the Phoenix Park, Dublin. Within Garda HQ, the main AFIS workstation environment will be located within the Garda Technical Bureau. AFIS servers and supporting database systems, are anticipated to be, located within Garda Headquarters.

All associated AFIS software modules will be located on this server environment.

Livescan/cardscan units and associated software integration components (with external agencies) may be deployed within a range of distributed environments (Garda stations, ports of entry, prisons and within ORAC itself).

Locations may include:

- Livescan/cardscan deployments at GNIB Headquarters in Burgh Quay, Dublin and approximately 23 Port of Entry and 90 district Garda stations located within the Irish Republic.
- ORAC livescan/cardscan deployment within ORAC asylum office at Lower Baggot Street, Dublin.
- Prison service livescan/cardscan deployments in MountJoy, Cork and Limerick Prisons.



**Note:** A final decision on the numbers of livescans and/or cardscans to be installed will be made during the analysis/business design phase of the implementation project. This decision will be based on a number of factors including cost, multi-function capability, environment and supporting hardware/network, usage requirements and profile.

### ***3.6.2 Security Clearance***

Suppliers should be aware that any person carrying out work on behalf of the Department of Justice, Equality and Law Reform or An Garda Síochána; on its premises or in relation to its data and information systems will require security clearance from An Garda Síochána before any work commences. Suppliers should be aware that this clearance process may be six to eight weeks in duration.

Accordingly, the successful supplier may be required to furnish An Garda Síochána with the name, address(s) and date of birth of all personnel assigned to the project as soon as the contract is awarded. The successful supplier may also be required to submit similar details in relation to additional personnel or changes in personnel occurring during the contract period.

Suppliers should confirm in their response that they will be able to comply with all security clearance procedures required by An Garda Síochána.

### ***3.6.3 Development Sites***

An Garda Síochána need to have very close links with the supplier's development and management team. This means meetings on a daily and/or weekly basis.

Suppliers are expected to locate project specific design & development teams in Garda Headquarters in Dublin.

Offices with furniture for a maximum of 25 people will be available for the project management team free of charge (but all project equipment and other requirements, e.g. telecommunication expenses, will be supplied by the successful supplier).

### ***3.6.4 Languages and Communication between Parties***

Suppliers must draft their tender offer in English. All deliverables, reports, draft and other documents must be delivered in English. Meetings will be conducted in English.

### ***3.6.5 Confidentiality***

Please note that the all tender documents and annexes are to be treated as confidential. Unauthorised disclosure by the supplier of any information to third parties received from the DJE&LR/An Garda Síochána in the process of this tender will result in its exclusion.

Suppliers are obliged to sign a declaration on confidentiality/non-disclosure (Appendix B) and return this immediately on receipt of the tender documentation.

### ***3.6.6 Paper version and CD-ROM version of Tender Documents***

In case of discrepancy between the paper version and CD-ROM version of the Tender Documents, the contents of the paper version shall prevail.



### 3.6.7 Contact Point and Clarifications

Whilst every endeavour has been made to inform accurately potential respondents of the requirements for this contract, suppliers should form their own conclusions about the methods and resources needed to meet those requirements. The Department of Justice, Equality and Law Reform/An Garda Síochána cannot accept responsibility for the bidder's assessment of the assignment.

Any queries concerning this document should be addressed to: [Eamonn.Murray@Garda.ie](mailto:Eamonn.Murray@Garda.ie)

The timetable below allows for three rounds of written queries during the response process. Answers to all queries will be circulated by email to all participating suppliers.

Round 1: Tender Queries (closing date)	March 16th
Round 1: Replies by	March 24th
Round 2: Tender Queries (closing date)	April 8th
Round 2: Replies by	April 15th
Round 3: Tender Queries (closing date)	April 22nd
Round 3: Replies by	April 27th
<b>Tender Closing Date:</b>	<b>May 9<sup>th</sup></b>

An Garda Síochána will endeavour to reply to all queries within the timeframes supplied above. All queries received by 5pm on the closing date for each round will be answered within the timeframe for that round.



## 4 SUBMISSION OF TENDERS

### 4.1 HOW TO SUBMIT TENDER OFFERS

Six (6) paper copies of the tender for this contract, plus two digital copies on CD (preferably in Word or Acrobat format) must be provided in a sealed package marked "Implementation and Integration of the National Fingerprint Identification System (AFIS) Contract" and addressed to:

Director of Finance,  
Tender Reception Office,  
An Garda Síochána,  
Garda Headquarters,  
Phoenix Park,  
Dublin 8,  
Ireland.

The tender must be delivered to reach the above address not later than 3pm on Monday May 9<sup>th</sup>, 2005. The name and contact details of the bidder should be clearly identified on the package.

Under no circumstances will tenders be accepted after the closing time and, no correspondence will be entered into regarding the delivery of tenders prior to the closing date time.

Suppliers are requested to make their own arrangements to obtain proof of delivery by, for example, obtaining a receipt.



## 5 LAYOUT AND CONTENT OF RESPONSES

Responses must be presented in the following format. Failure to do so may result in rejection of the tender.

### Chapter 1 Executive Summary

This chapter must introduce the general capacity and technical capability of the supplier that will fulfil the contract, including roles of all sub-contractors and/or product suppliers in a consortium. Any sub-contracting arrangements must be described.

The executive summary must include, at a minimum:

- An overview of the supplier's understanding of the requirements.
- A summary of the proposed solution, highlighting the most important features of the solution and services proposed.
- An outline of the general approach and plans regarding the analysis, design, systems development, testing, training, documentation and implementation of the proposed solution.
- A brief outline of the approach and plans for the ongoing support of the systems.
- A summary of the costs.

### Chapter 2 Administrative Information

The response document for the contract must identify the name, postal and e-mail address, telephone and fax number of the supplier and the name of the person within the supplier business dealing with the contract.

The tender must be hosted by a nominated prime contractor, pre-qualified from the previous stage of this procurement. The solution offered for the contract may involve the provision of services from either a single party or a group/consortium of suppliers. Where a particular bid for the contract is based on a group/consortium of business interests, the tender response document must identify:

- The pre-qualified nominated prime contractor in the group/consortium.
- The number of parties involved and the names of each.
- The proposed arrangements for its operation, e.g. the area of participation of each party in the context of the contract.

Where a bid from a group or consortium of suppliers succeeds in respect of the contract, the Department of Justice, Equality and Law Reform/An Garda Síochána will conclude a contract with the pre-qualified prime contractor only who will then take sole responsibility for all matters arising under that contract.

In addition to the information already given in the request to participate (selection process), the supplier must provide any changes or new administrative information relevant for the project.

Confirmation of acceptance of all points raised in this document in sections **Additional Information, Conditions of Tender and Contractual Matters**.

### Chapter 3 Response to Functional Requirements

Suppliers must provide an overview of how their solution will meet all of the functional requirements specified in Chapter 5 of **Section B: Requirements Specification**. In addition they must respond as follows:

- FC (Fully compliant): 100% compliant to requirement.





- PC (Partially Compliant): A result close to the desired outcome is achieved or an alternative solution is proposed (a manual or semi-automated solution exists).
- NC (Not compliant): Supplier solution does not have a solution to the requirement.

To each of the requirements as detailed in **Appendix B 1 – Functional Requirements of Section B: Requirements Specification.**

#### **Chapter 4 Response to Integration Requirements**

Suppliers must provide an overview of how their solution and systems architecture will meet all of the integration requirements specified in Chapter 6 of **Section B: Requirements Specification.** In addition they must respond as follows:

- FC (Fully compliant): 100% compliant to requirement.
- PC (Partially Compliant): A result close to the desired outcome is achieved or an alternative solution is proposed (a manual or semi-automated solution exists).
- NC (Not compliant): Supplier solution does not have a solution to the requirement.

To each of the requirements as detailed in **Appendix B 2 – Integration Requirements of Section B: Requirements Specification.**

#### **Chapter 5 Response to Security Requirements**

Full response to all points raised in Chapter 7 of **Section B: Requirements Specification.**

#### **Chapter 6 Response to Infrastructure Requirements**

Full response to all points raised in Chapter 8 of **Section B: Requirements Specification.**

#### **Chapter 7 Response to System Requirements**

Full response to all points raised in Chapter 9 of **Section B: Requirements Specification.**

#### **Chapter 8 Response to Hardware Requirements**

Full response to all points raised in Chapter 10 of **Section B: Requirements Specification.**

#### **Chapter 9 Response to Site Requirements**

Full response to all points raised in Chapter 12 of **Section B: Requirements Specification.**

#### **Chapter 10 Approach to Delivery and Support**

Full response to all points raised in Chapter 13 of **Section B: Requirements Specification.** In particular the phases of work should be clearly broken out and identified in compliance with the principle that the core AFIS system replacement work will remain unhindered by all parallel or subsequent work streams.

#### **Chapter 11 Response to Support Requirements**

Full response to all points raised in Chapter 14 of **Section B: Requirements Specification.**

#### **Chapter 12 Costing Document**

- The schedule of costs must provide full details in respect of all costs which would be incurred for services and facilities offered over the duration of the project and should, where possible, follow the general format set out in Appendix A – Schedule of Costs.



- The content of each table may be adapted to reflect the particular manner in which costs would be incurred e.g. additional rows may be added to itemise individual items, services and separately licensable facilities.
- The name and version/release number of each product being costed should be inserted under the 'Cost Item' column. Where separately licensable items are offered, the licence costs for each should be itemised separately therein.
- Where elements offered are not an essential or an integral part of the solution, they should be clearly identified as such and marked as 'Optional'.
- Fixed pricing is required in respect of all elements of the Contract. Accordingly, where expenses or other incidental costs would be incurred, these must now be quantified and incorporated in the fixed pricing disclosed in the Schedule.
- The supplier must provide for each component of the solution a breakdown of days per role type, the daily rate and the overall cost of each component. The overall cost of each element must be broken down by design, development, project management and implementation costs are required for each component of the solution as illustrated in Appendix A – Schedule of Costs. It is vital that the supplier clearly separate the costs of the overall solution so as to allow for modular purchase of each phase of the implementation.
- The supplier must provide details of staged payments schedule and illustrate which key milestones will be linked to payments, an example is included in Appendix A – Schedule of Costs.
- Similarly, support and maintenance costs must be quantified on an annual basis. Where on-going costs differ from year-to-year, they should be itemised for each year e.g. add a separate column for Year 1, Year 2 and Year 3.
- All costs must be quoted in Euro currency denominations (€), exclusive of VAT. The applicable rate of VAT and any other taxes, or duties, which would be incurred should be itemised separately.
- The supplier must provide daily rates per resource type for each of the next 3 years and illustrate any discounting options available.
- Suppliers *must include costs for all equipment* (PCs, servers, hubs, switches, network cards, livescan units, computer peripherals etc) which will be necessary to implement the solution. However, where unforeseen equipment purchases arise, the supplier must specify in their response the arrangement they will make to allow for the purchase of this additional equipment (e.g. a set handling cost percentage or expense to be applied to original invoices).
- The supplier must provide a detailed breakdown of every individual software and hardware item proposed for the solution. Details should be included as an appendix to the ITT response:
  - ✓ **Appendix C**      Hardware Catalogue: Technical details of all hardware proposed
  - ✓ **Appendix D**      Software Catalogue: Technical details of all COTS software proposed

The costing document should be bound under a separate cover to the main response.

#### Summary of Annexes to Accompany the Response:

- Annex A**      Completed Schedule of Costs.
- Annex B**      Signed declaration of confidentiality.
- Annex B 1**    Completed Appendix B 1– Functional Requirements.



- 
- Annex B 2** Completed Appendix B 2 – Integration Requirements.
- Annex C** Hardware Catalogue: Technical details of all hardware proposed.
- Annex D** Software Catalogue: Technical details of all COTS software proposed.



## 6 EVALUATION OF TENDERS & AWARD CRITERIA

Tenders must be submitted in the English language and hosted by a prime contractor pre-qualified for this contract from the earlier stage in the procurement process.

Tenders will be initially examined for responsiveness of proposal i.e. the tender must address all of the requirements, include all information requested and comply with the format of responses requested in this Invitation to Tender and its subsections. Only tenders which address the requirements stated in this document will be considered for the award process.

Any contract will be awarded from the responsive tenders on the basis of An Garda Síochána's assessment of the most economically advantageous tender applying the following award criteria, listed in order of priority:

- a) The technical merit, functional fit and organisational value of the solution offered. This will include an assessment of the functionality offered, the merits and consequences of the technical architecture and the performance features and characteristics of the solution (350 marks).
- b) Costs. An Garda Síochána will endeavour to calculate costs on a like-for-like basis. All annual or recurring costs will be calculated over a 3 year period (250 marks).
- c) The quality and extent of the full range of services offered to develop and implement the solution. This will include an assessment of the skills, experience and expertise of the proposed personnel and an evaluation of the nature of the processes and procedures, which will be deployed by the supplier's team to ensure that all aspects of the solution will be delivered to a very high quality standard (200 marks).
- d) The quality and extent of the post-implementation support offered (150 marks).
- e) The future development plans of the developer/manufacturer for the key elements of the solution (50 marks).

### 6.1 EVALUATION PROCESS

As part of the evaluation of the Technical Merit and Functional Fit of the solution, An Garda Síochána, at its discretion, may wish to perform an assessment of the vendor products and solutions.

An Garda Síochána may also wish to interview the key personnel proposed by the supplier for the contract. Accordingly, respondents must be in a position to make such personnel available for interview, at reasonable notice, if so requested. It is intended that such interviews would be held in An Garda Síochána's premises in Dublin.

Respondents will be required to bear their own costs in respect of any such interviews and/or demonstrations and benchmarking.

Arrangement for benchmarking, presentations or demonstrations will be notified to the suppliers during the evaluation phase of the process.



## 7 CONDITIONS OF TENDER

Detailed contractual arrangements are not within the scope of this document. However, the following conditions apply to the competition and should be noted, and where appropriate, responded to in the document.

The Department of Justice, Equality and Law Reform reserves the right to seek clarification of any information provided in the bidder's tender.

The awarding authority will not be liable for any costs incurred by respondents in the preparation, submission or presentation of applications or tenders, or any associated work or effort howsoever incurred.

Whereas this document is issued in good faith, no legitimate expectation shall arise there from and the Department shall not be obliged to award a contract or proceed to further stages in the procurement process.

Before contracts are awarded the successful contractors (prime and sub-contractors) will be required to comply with the prevailing tax clearance procedures viz:

- A successful contractor resident in Ireland will be required to promptly produce a Tax Clearance Certificate from the Irish Revenue Commissioners.
- A successful non-resident contractor will be required to produce a statement (in lieu of a Tax Clearance Certificate) from the Irish Revenue Commissioners confirming suitability on tax grounds to be awarded the contract.

Where a certificate or statement expires during the course of the contract, the Department will require a renewed certificate or statement. All payments under the contract will be conditional on contractors being in possession of valid certificates at all times.

In responding to this document, all applicants (prime and sub-contractors) should state that their tax affairs are in order and that obtaining a Tax Clearance Certificate or Statement of Suitability from the Irish Revenue Commissioners will not pose a problem for them.

Any conflicts of interest involving a contractor must be fully disclosed to the Department, particularly where there is a conflict of interest in relation to any recommendations or proposals put forward by the supplier. Any "registerable interest" involving the contractor and the Minister for Justice, Equality and Law Reform, members of the Government, members of the Oireachtas (parliament) or employees of the Department of Justice, Equality and Law Reform or their relatives must be fully disclosed in the response to this Invitation to Tender or should be communicated to the Department of Justice, Equality and Law Reform immediately upon such information becoming known to the contractor, in the event of this information only coming to their notice after the submission of a bid and prior to the award of the contract. The terms "registerable interest" and "relative" shall be interpreted as per Section 2 of the Ethics in Public Office Act, 1994.

The successful contractor for the contract will be obliged to pay subcontractors in accordance with the relevant applicable provisions of the Prompt Payment of Accounts Act 1997 (No 31 of 1997), as amended.

The awarding authority undertakes to hold confidential any information provided by candidates in their response documents, subject to its obligations under law, including the Freedom of Information Acts 1997 and 2003.

Note that under the Freedom of Information Acts, information provided by suppliers may be liable to be disclosed where the public interest value of releasing such information is deemed to outweigh the right to confidentiality. The Department will consult with the party supplying confidential information before making any decision on releasing such information in response to a request under the Acts.

Suppliers are asked to consider if any of the information supplied by them in their response document should not be disclosed because of its sensitivity. If this is the case, the supplier should when providing the information, identify same and specify the reasons for its sensitivity. If the supplier does not identify it as sensitive and the Department,

Implementation and Integration of The National Fingerprint Identification System. Section A: Administrative Instructions.



on consideration, do not deem it sensitive then it is liable to be released in response to a Freedom of Information Act request without further consultation with the supplier. The Department will consult with the supplier about sensitive information before making a decision on a request that it receives pursuant to the Freedom of Information Acts.

If the supplier considers that none of the information supplied is sensitive please make a statement to that effect. Such information is liable to be released in response to a Freedom of Information Act request.



## 8 CONTRACTUAL MATTERS

Work under this contract would be expected to commence promptly following the award of contract which is, at present, scheduled for May 2005.

Any contract concluded under this procurement will be governed by Irish law and, subject to arbitration provisions, the parties will submit to the exclusive jurisdiction of the Irish Courts.

As provided by "EU Council Directive 2004/18/EC (March 31<sup>st</sup>)", the awarding authority reserves the right to adopt the negotiated procedure to engage the successful contractor from this procurement to undertake new services consisting in the repetition of similar services which conform to this basic project, in accordance with the said Article.

Whereas detailed contractual arrangements are beyond the scope of this document, it is intended that the tender documents submitted by the successful bidder, and all subsequent clarifications and presentations, will be referenced in, and form part of, the final contract.

It is also anticipated that any contract entered into with the supplier will include provisions relating to the following:

- Intellectual Property Rights (IPR) in new and existing software.
- Liability arising from failure of the contractor to perform its obligations under the contract. The successful contractor will be required to hold appropriate professional risk indemnity insurance, or equivalent insurance, covering such liabilities, throughout the duration of the contract.
- A clause indemnifying the Department of Justice, Equality and Law Reform and An Garda Síochána from liability for any injuries or loss incurred by the contractor's employees, sub-contractors, servants and agents while present on Department's premises.
- Contract provisions will include milestone payments, retention payment, and penalties for non-performance or late delivery.
- Appropriate 'Force Majeure' provisions.
- Confidentiality of trade secrets and professional secrets relevant to the performance of the contract.
- Position and obligations of the respective parties under the prevailing Data Protection legislation.
- Change control procedures. Please note that all changes to the operation of the project will be conducted through formal change control procedures which would be agreed between the contractor and the AFIS Project Board.
- Change of Key Personnel. It will be a condition of contract that all key personnel to be associated with the project, as proposed in the Tender, are listed in the contract documents. Where such personnel become incapacitated or otherwise unavailable, the supplier shall propose alternate staff of at least equal qualifications, experience and expertise for approval by the AFIS Project Board, which approval shall not be unreasonably withheld. Failure to provide an acceptable replacement promptly may result in the Department of Justice, Equality and Law Reform terminating the contract.

Suppliers should note that the above list is not intended to be exhaustive. Contractual discussions will be undertaken, in due course, with the bidder adjudged to have submitted the most economically advantageous tender.

Implementation and Integration of The National Fingerprint Identification System. Section A: Administrative Instructions.



---

**9 APPENDIX A - SCHEDULE OF COSTS**





## 10 APPENDIX B - DECLARATION ON CONFIDENTIALITY

### DECLARATION ON CONFIDENTIALITY AND NO CONFLICT OF INTEREST

Compulsory Form to be filled in and signed by each member of the supplier's invitation to tender team

- 1) I, \_\_\_\_\_, agree not to disclose any classified, sensitive or proprietary information that is presented, discussed or made accessible during my participation in the 'Implementation and Integration of the National Fingerprint Identification System' invitation to tender, to any person or legal entity who has not signed a nondisclosure agreement.

I understand that information I may become aware of, or possess, as a result of this access is considered proprietary or sensitive. I agree not to appropriate such information for my own use or to release or disclose it to third parties unless specifically authorised to do so. I also understand that I must protect proprietary information from unauthorised use or disclosure for as long as it remains proprietary and refrain from using the information for any purpose other than that for which it was furnished.

I continue to be bound by this undertaking after completion of the 'Implementation and Integration of the National Fingerprint Identification System' invitation to tender procedure.

I understand that a violation of this agreement is subject to administrative, civil and criminal sanctions.

- 2) I declare that in relation to the 'Implementation and Integration of the National Fingerprint Identification System' invitation to tender procedure, I am not placed in a situation that could give rise to conflict of interests, in particular as a result of economic interest, political or national affinity, family or emotional ties, or any other relevant connection or shared interest.

\_\_\_\_\_  
Printed Name

\_\_\_\_\_  
Institution or Company

\_\_\_\_\_  
Address, E-Mail and Phone Number

\_\_\_\_\_  
Place and Date

\_\_\_\_\_  
Signature

**Mary Mc Donald**

---

**From:** Helen Costello  
**Sent:** 30 August 2005 10:41  
**To:** Mary Mc Donald  
**Subject:** RE: T.61/2005 Implementation & integration of the National Identification System

Mary,

These tenders are still being evaluated,.....will take a few months!

Helen

---

**From:** Mary Mc Donald  
**Sent:** 30 August 2005 10:26  
**To:** Helen Costello  
**Subject:** T.61/2005 Implementation & Integration of the National Identification System

Helen-

Just looking for an update on this file. Closed on 9 May 2005.

Regards

Mary

**Mary Mc Donald**

---

**From:** Mary Mc Donald

**Sent:** 30 August 2005 10:26

**To:** Helen Costello

**Subject:** T.61/2005 Implementation & integration of the National Identification System

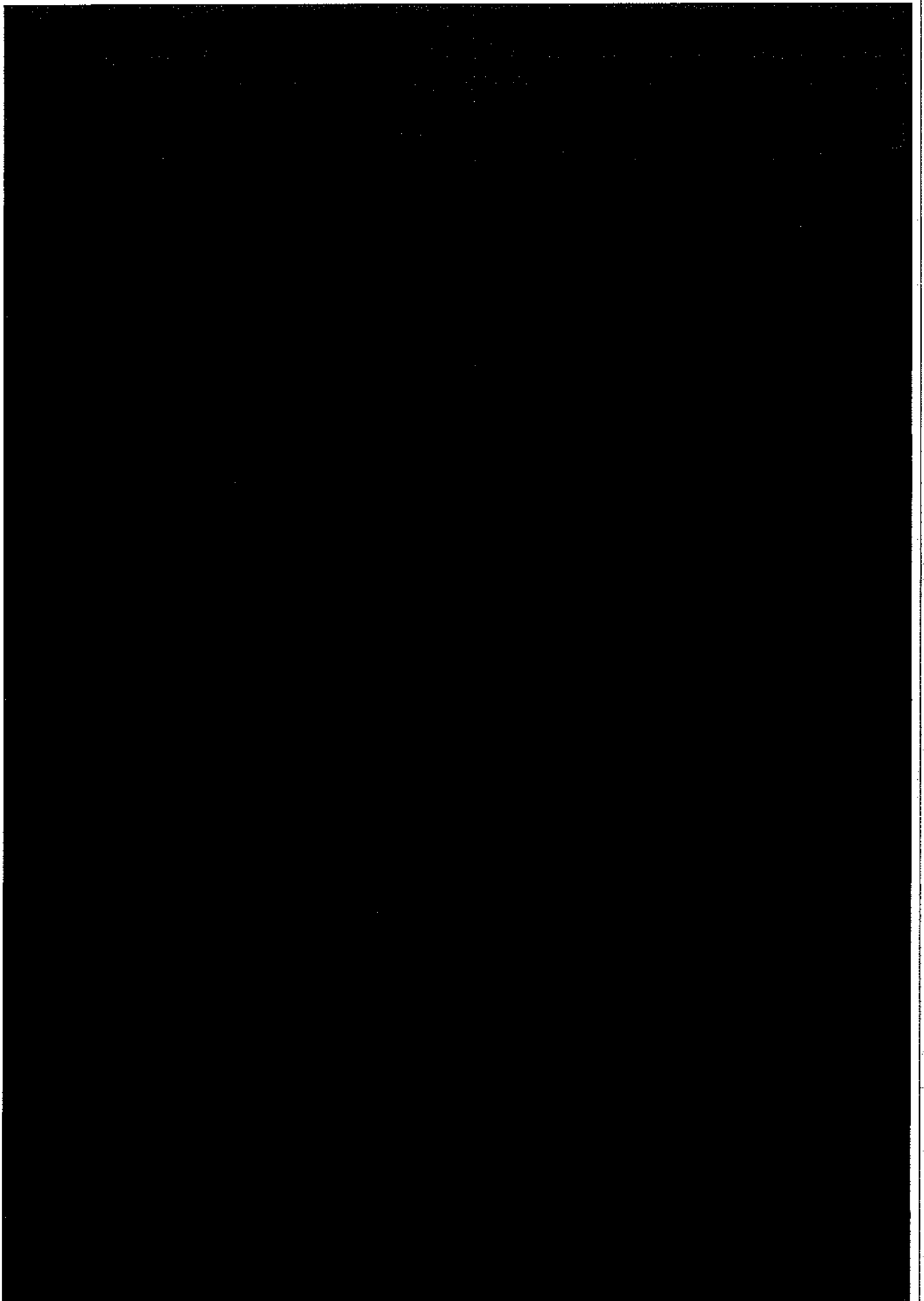
Helen-

Just looking for an update on this file. Closed on 9 May 2005.

Regards

Mary

30/08/2005



CHANNELS [Careers](#) - [Finance](#) - [Entertainment](#) - [News](#) - [Sport](#) - [Lettings](#) - [Shop](#)  
COMMUNICATE [Email](#) - [SMS](#) - [Chat](#) - [My Mobile](#)  
SERVICES [Music and DVDs](#) - [Dating](#)



• W  
• K  
• R  
• b

[Check for Mail](#) [Create Message](#) [Mail Folders](#) [Empty Trash](#) [Address Book](#) [My Settings](#) [Help](#)



READ 1

[Prev message](#) [Next message](#) [Inbox/New Mail](#) [Reply](#) [Reply-All](#) [Forward Message 1 of 6](#)

**From:** Helen Costello <Helen.Costello@garda.ie>

**Subject:** Qry re Delivery of Teder

**CC:** Fintan Fanning <Fintan.Fanning@Garda.ie>

**Date:** Thu, 5 May 2005 15:52:02 +0100

**Attachments:**

Mary,

Following our conversation re a tender to be delivery on Mon 9th May.

The following is an extract from the tender "Implementation and Integration of the National Fingerprint Identification System (AFIS) Contract ", due in Mon 9th May 2005. Your office down as place of delivery. It was a restricted tender. There should be 5 submissions

I am available at [redacted] and will be available on Monday 9th.

Thanks

Helen

**Submission Of Tenders**

**How to submit Tender Offers**

Six (6) paper copies of the tender for this contract, plus two digital copies on CD (preferably in Word or Acrobat format) must be provided in a sealed package marked "Implementation and Integration of the National Fingerprint Identification System (AFIS) Contract "and addressed to:

Director of Finance,  
Tender Reception Office,  
An Garda Síochána,  
Garda Headquarters,  
Phoenix Park,  
Dublin 8,  
Ireland.

The tender must be delivered to reach the above address not later than 3pm on Monday May 9th, 2005. The name and contact details of the bidder should

be clearly identified on the package.  
Under no circumstances will tenders be accepted after the closing time and, no correspondence will be entered into regarding the delivery of tenders prior to the closing date time.  
Suppliers are requested to make their own arrangements to obtain proof of delivery by, for example, obtaining a receipt.

\*\*\*\*\*  
The information transmitted is intended only for the person or entity to which it is addressed and may contain confidential and/or privileged material. Any review, retransmission, dissemination or other use of, or taking of any action in reliance upon, this information by persons or entities other than the intended recipient is prohibited.

If you received this in error, please contact the sender and delete the material from any computer. It is the policy of An Garda Síochána to disallow the sending of offensive material and should you consider that the material contained in this message is offensive you should contact both the sender and [postmaster@garda.ie](mailto:postmaster@garda.ie) immediately.

\*\*\*\*\*

[Prev message](#) [Next message](#) [Inbox/New Mail](#) [Reply](#) [Reply-All](#) [Forward](#) Message 1 of 6

---

Move to folder	Inbox	Delete	Set View Style
<input type="checkbox"/> View headers	<input type="checkbox"/> Variable width font	<input checked="" type="checkbox"/> Inline Images	
<input type="checkbox"/> View as HTML	<input type="checkbox"/> Execute HTML		



**eTenders Public Procurement**  
The website for Irish public tenders

[Notice Search](#) | [Publish Notice](#) | [Register](#) | [Sign In](#) | [News](#) | [Guides](#) | [About Us](#) | [Site Help](#)

v1.1.5.0

- Authority**
- Home
  - **Create Notice**
  - Notice Workspace
  - Organisation Details
  - Your Details
  - Library

- Quick Links**
- Site Home Page
  - Notice Search
  - Authority Search
  - Register
  - Supplier Home
  - Authority Home
  - Publish Notice
  - News
  - Guides
  - Links
  - About Us
  - Site Help

**Gaeilge**

**Notice Status**

Notice Wizard Details

**Document ID:** 7275 [View the original text](#)

**Title:** National Fingerprint Identification System

**Type of Document:** OJEU Notice

**Type of Notice:** Contract Notice

**Services/Supplies:** Supply Contract

**Procedure Type:** Restricted Procedure

**Is Accelerated:** No

**Is Utility:** No

**Document Source:** OJEU Wizard

**Status:** Dispatched

**Created:** 15-Dec-04 15:13 by Peter Lumsden

**Last Amended:** 16-Dec-04 16:47 by Peter Lumsden

**Released:** 16-Dec-04 16:54

**Published:** 16-Dec-04 16:55 by Peter Lumsden  
Ref: DEC031407 ( XMLID=5822, Mail=IE001-XML05-20041216)

Published Details

Garda Siochana

**Type of Notice:** Tenders

**Document Source:** EU Wizard

**Status:** Active

**Created:** 16-Dec-2004 16:55 by Peter Lumsden

**Published:** 16-Dec-2004 00:00

**Verified:** 16-Dec-2004 16:55

**Last Amended:** 17-Dec-2004 11:45 by Peter Lumsden

**Embargoed:** -

**Application Deadline:** -

**Tender Deadline:** 04-Feb-2005 at 15:00 [Change](#) | [Cancel](#)

**Archived Date:** -

**Has Further Information:** Yes, 4, [View/Change List of Further Information](#)

**Has Documents:** Yes, 1, [View/Change Additional Document List](#)

**Has Noted Interests:** Yes, 63, [View/Change Noted Interest List](#)

---

The following can access the noted interest area:  
[Change](#)

**Has Additional Logos:** No, [View Additional Logo List](#)  
**Has Postbox:** No

---

[Home Page](#) | [Contact Us](#) | [Help](#) | [Terms & Conditions](#) | [Privacy Policy](#)





v1.1.5.0

[Notice Search](#) | [Publish Notice](#) | [Register](#) | [Sign In](#) | [News](#) | [Guides](#) | [About Us](#) | [Site Help](#)
**Authority**

- Home
- Create Notice
- Notice Workspace
- View Interest
- Create Further Info
- Change deadlines
- Cancel Notice
- Print Notice
- Authority Dets
- Your Details
- Library

**Quick Links**

- Site Home Page
- Notice Search
- Authority Search
- Register
- Supplier Home
- Authority Home
- Publish Notice
- News
- Guides
- Links
- About Us
- Site Help

**Gaeilge****View Published Notice**

Details of the published notice are shown below. If you wish to publish further information regarding this notice please select the **Create Further Info** link from the menu.

Title: National Fingerprint Identification System for An Garda Siochana

Awarding Authority: Department of Justice, Equality and Law Reform

Publication date: 16-Dec-2004

Application Deadline:

Tender Deadline Date: 04-Feb-2005

Tender Deadline Time: 15:00

Notice Type: Tenders

Has Documents: Yes

**Abstract:** The purpose of this document is to provide background and briefing material for parties interested in responding to the advertisement for a new National Fingerprint Identification System for An Garda Siochana. It does not constitute a detailed or final specification of requirements for the contract in question. The material herein is intended to provide interested parties with sufficient information to prepare their response document for this pre - qualification stage, and will be superceded by the requirements of the Invitation to Tender document which will issue in due course.

**Additional Documents**

Description	Name	Size
National Fingerprint Identification System for An Garda Siochana	V2 of EU AFIS DOC.doc	318464
AFIS Questions	afis questions.doc	31744
AFIS Q & A Part II	AFIS Q and A Part II.doc	27136

**Contact Information**

Main Contact: [info@justice.ie](mailto:info@justice.ie)

Admin Contact: [fintan.fanning@garda.ie](mailto:fintan.fanning@garda.ie)

Technical Contact: N/a

Other Contact: N/a

**Full Notice Text****CONTRACT NOTICE**

Notice Type: SUPPLIES

Is this contract covered by the Government Procurement Agreement (GPA)? Yes

### SECTION I: CONTRACTING AUTHORITY

#### I.1) Official Name and Address of the Contracting Authority

<b>Organisation</b> Department of Justice, Equality and Law Reform	<b>For the attention of</b> Garda Planning Division
<b>Address</b> Garda Planning Division , 94 St. Stephen's Green, Dublin 2	<b>Postal Code</b> 2
<b>Town</b> Dublin	<b>Country</b> IE
<b>Telephone</b> 01 4086106	<b>Fax</b> 4086142
<b>Electronic Mail</b> info@justice.ie	<b>Internet Address (URL)</b> www.justice.ie

#### I.2) Address from which further information can be obtained

As in I.1  *If different, see Annex A*

#### I.3) Address from which documentation may be obtained

As in I.1  *If different, see Annex A*

#### I.4) Address to which Tenders/Requests to participate must be sent

As in I.1  *If different, see Annex A*

#### I.5) Type of contracting Authority

Central Level  EU Institution  Other   
Regional/local Level  Body governed by public law

### SECTION II: OBJECT OF THE CONTRACT

#### II.1) Description

II.1.1) Type of works contract

II.1.2) Type of supplies contract

Purchase  Rent  Lease   
Hire-purchase  Combination of these

II.1.3) Type of service contract

II.1.4) Is it a framework agreement:  
No

II.1.5) Title attributed to the contract by the contracting authority  
National Fingerprint Identification System for An Garda Siochana

II.1.6) Description/object of the contract

The purpose of this document is to provide background and briefing material for parties interested in responding to the advertisement for a new National Fingerprint Identification System for An Garda Siochana. It does not constitute a detailed or final specification of requirements for the contract in question. The material herein is intended to provide interested parties with sufficient information to prepare their response document for this pre - qualification stage, and will be superseded by the requirements of the Invitation to Tender document which will issue in due course.

NOTE: Further information relating to this notice is available on the eTenders Web Site at  
[http://www.etenders.gov.ie/Search/Search\\_Switch.aspx?ID=7275](http://www.etenders.gov.ie/Search/Search_Switch.aspx?ID=7275).

- II.1.7) Site or location of works, place of delivery or performance  
Ireland  
NUTS Code IE
- II.1.8) Nomenclature
- II.1.8.1) Common Procurement Vocabulary (CPV)
- |                    |                    |   |
|--------------------|--------------------|---|
|                    | Main<br>vocabulary | Supplementary vocabulary ( <i>when<br/>applicable</i> ) |
| Main object        | <b>72540000</b>    |   |
| Additional objects |                    |   |
- II.1.8.2) Other relevant nomenclature (CPA/CPC)
- II.1.9) Division into lots  
No
- II.1.10) Will variants be accepted  
No
- II.2) Quantity or Scope of the Contract**
- II.2.1) Total quantity or scope
- II.2.2) Options. Description and time when they may be exercised
- II.3) Duration of the contract or limit for completion**

**SECTION III: LEGAL, ECONOMIC, FINANCIAL AND TECHNICAL INFORMATION**

- III.1) Conditions Relating to the Contract**
- III.1.1) Deposits and guarantees required
- III.1.2) Main Terms of financing and payment and/or reference to the relevant provisions
- III.1.3) Legal form to be taken by the grouping of suppliers, contractors or service providers to who legal contract is awarded
- III.2) Conditions for Participation**
- III.2.1) General Conditions
- III.2.1.1) Legal Position - means of proof required
- III.2.1.2) Economic and Financial Capacity- means of proof required
- III.2.1.3) Technical Capacity- means of proof required

**SECTION IV: PROCEDURE****IV.1) Type of Procedure**

- |            |                                     |                        |                          |
|------------|-------------------------------------|------------------------|--------------------------|
| Open       | <input type="checkbox"/>            | Accelerated Restricted | <input type="checkbox"/> |
| Restricted | <input checked="" type="checkbox"/> | Accelerated Negotiated | <input type="checkbox"/> |
| Negotiated | <input type="checkbox"/>            |                        |                          |

- IV.1.1) Have candidates already been selected?  
No
- IV.1.2) Justification for the choice of accelerated procedure.
- IV.1.3) Previous publication concerning the same contract
- IV.1.3.1) Prior information notice concerning the same contract  
Notice Number 2004/S 551-043631 of 12-03-2004
- IV.1.3.2) Other previous publications
- IV.1.4) Envisaged number of suppliers which will be invited to tender  
Minimum: 5 / Maximum: 8
- IV.2) Award Criteria**
- A) Lowest Price No
- B) The most economically advantageous tender in terms of:
- B1) Criteria as stated below No
- B2) Criteria as stated in contract documents: Yes

**IV.3 Administrative Information**

- IV.3.1) Reference number attributed to the notice by the contracting authority  
AFIS
- IV.3.2) Conditions for obtaining contract document and additional documents  
Obtainable until
- Price *(where applicable)* Currency
- Terms and method of payment
- IV.3.3) Time-limit for receipt of tenders or requests to participate  
04-02-2004 Time *(when applicable)* 15:00
- IV.3.4) Dispatch of invitations to tender to selected candidates  
Estimated date 01-04-2004
- IV.3.5) Language or languages in which tenders or requests to participate can be drawn up  
EN
- IV.3.6) Minimum time frame during which the tenderer must maintain its tender
- IV.3.7) Conditions for opening tenders
- IV.3.7.1) Persons authorised to be present at the opening of tenders *(where applicable)*
- IV.3.7.2) Date, time and place
- Date Time  
Place

**SECTION VI: OTHER INFORMATION**

- VI.1) Is this notice a Non Mandatory one?  
No
- VI.2) Indicate Whether this Procurement is a Recurrent one and the Estimated Timing for Further Notices to be Published
- VI.3) Does the contract relate to a Project/Programme financed by EU Funds?  
No  
*If yes, indicate the project/programme and any useful reference*
- VI.4) Additional Information  
(ET Ref:7275)
- VI.5) Dispatch date of this Notice  
16-12-2004

**ANNEX A**

- I.2) Address from which further information can be obtained

<b>Organisation</b> Garda Siochana ( Police ) Headquarters	<b>For the attention of</b> Flintan Fanning
<b>Address</b> Phoenix Park, Dublin, 8.	<b>Postal Code</b> Dublin,8.
<b>Town</b> Dublin	<b>Country</b> IE
<b>Telephone</b> 0035316660000	<b>Fax</b> 0035316662419
<b>Electronic Mail</b> flintan.fanning@garda.ie	<b>Internet Address (URL)</b> www.garda.ie

**1.3) Address from which documentation may be obtained**

<b>Organisation</b> Garda Síochána ( Police ) Headquarters	<b>For the attention of</b> Flintan Fanning
<b>Address</b> Phoenix Park, Dublin, 8.	<b>Postal Code</b> Dublin 8
<b>Town</b> Dublin 8	<b>Country</b> IE
<b>Telephone</b> 0035316660000	<b>Fax</b> 0035316662419
<b>Electronic Mail</b> flintan.fanning@garda.ie	<b>Internet Address (URL)</b> www.garda.ie

**1.4) Address to which Tenders/Requests to Participate must be sent**

<b>Organisation</b> An Garda Síochána	<b>For the attention of</b> Director of Finance
<b>Address</b> Tender Reception Office, Garda Headquarters, Phoenix Park	<b>Postal Code</b> Dublin,8
<b>Town</b> Dublin 8	<b>Country</b> IE
<b>Telephone</b> 0035316660000	<b>Fax</b> 0035316662419
<b>Electronic Mail</b>	<b>Internet Address (URL)</b>

## Further Information

Information added to the notice since publication.

**17-Dec-2004 Deadline Date(s) Changed**

The deadline date was changed from 04-Feb-2004 to 04 Feb 2005,  
error in entering the date

17-Dec

**National Fingerprint Identification System for An Garda Síochána**

Background and briefing material for parties interested in responding to the advertisement for the new system

27-Jan-2005 FAQ's

List of Questions received pursuant to 6.4 of supporting documents REF DEC031407 titled National Fingerprint Identification System for An Garda Síochána

01-Feb-2005 AFIS Questions and Replies - Part 2

Clarification and Responses - Part

[Home Page](#) | [Contact Us](#) | [Help](#) | [Terms & Conditions](#) | [Privacy Policy](#)



**Implementation and Integration of the National Fingerprint  
Identification System**

**For**

**An Garda Síochána,  
The Department of Justice, Equality and Law Reform  
And  
The Office of Refugee Applications Commissioner (ORAC).**

**Briefing Document  
(Pre-qualification stage)**

**Date: 14<sup>th</sup> December, 2004**

# National Fingerprint Identification System

## Briefing Document

### Table of Contents

1. Purpose of Document.....	3
2. Organisation & Project Background .....	4
Organisation Background .....	4
Fingerprint Project Background.....	7
3. Overview of Existing National Fingerprint Identification Systems .....	9
Existing AFIS Support Process Overview.....	9
Installed AFIS Technical Overview .....	10
Future Solution Overview.....	11
Key components .....	11
Systems Integration .....	11
4. Preliminary Outline of Requirements.....	13
5. Procurement Process .....	18
6. Administrative Arrangements.....	19
7. Notices and Conditions.....	20
8. Material Required in Response Document.....	22
Response material required.....	22
Response Section A: General Information .....	22
Response Section B: Suppliers Financial and Economic Standing .....	22
Response Section C: Suppliers Technical Capability .....	23
Evaluation Criteria.....	24

## 1. Purpose of Document

The purpose of this document is to provide background and briefing material for parties interested in responding to the pre-qualification advertisement for a new National Fingerprint Identification System for An Garda Síochána, as published in the Supplement to the Official Journal of the European Communities. An Garda Síochána is the National Police Force in the Republic of Ireland responsible for all aspects of criminal law enforcement and national security. An Garda Síochána has a central Headquarters based at The Phoenix Park, Dublin 8. Further information on An Garda Síochána is available on the website at <http://www.garda.ie/>.

A Prior Information Notice for the project was published previously on 12/03/2004 Reference: 2004/S 51-043631.

This briefing document relates to the Contract for a complete system comprising:

- Hardware.
- Software.
- Development.
- Implementation.
- Integration with existing systems and,
- Long-term support services as an option to be exercised solely at the discretion of An Garda Síochána.

This briefing document does *not* constitute a detailed or final specification of requirements for the contract in question. The material herein is intended to provide interested parties with sufficient information to prepare their response document for the **pre-qualification** stage (see Section 5: for further details). The material herein will be superseded by the detailed requirements to be specified within the Invitation to Tender document, which will issue in due course to those service providers (suppliers) selected to bid for this contract from this pre-qualification stage.



## 2. Organisation & Project Background

This section provides background to the relevant organisations and processes.

### Organisation Background

#### (a) Asylum and Immigration

The Department of Justice, Equality and Law Reform is responsible for the development the Government's asylum and immigration policies and strategies. A number of Divisions of the Department and Agencies implement these policies on behalf of the Minister.

For the purposes of this briefing, the relevant agencies/ offices involved in the various processes are the Office of the Refugee Applications Commissioner (responsible for asylum) and the Garda National Immigration Bureau (responsible for immigration). The AFIS functions (currently for Asylum and in the future GNIB) are provided by the Garda Technical Information Bureau (GTB) with support for both GNIB and GTB provided by the Garda Information Technology Division.

#### (b) Criminal Fingerprinting

This is primarily the responsibility of An Garda Síochána with the Garda Technical Information Bureau (GTB) providing the key role. Prints are captured at Garda Stations and submitted to the GTB for processing and storage. Prints are taken manually except in two locations that use livescan units.

Capture of prints using one livescan unit also takes place in the Irish Prisons Service and are electronically transmitted to the GTB.

The following are further details of the specific Agencies / Divisions involved.

#### *The Office of the Refugee Applications Commissioner*

The Office of the Refugee Applications Commissioner (ORAC) is the first instance decision-making body in the Irish asylum system. The office was established under the Refugee Act, 1996 (as amended). Under the Act, the Commissioner is required to investigate each asylum application lodged within the state and to make recommendations to the Minister for Justice, Equality and Law Reform. The Commissioner is also responsible for investigating applications by refugees to allow family members to enter and reside in the State and for providing a report to the Minister on such applications. The Commissioner is independent in the exercise of his or her functions.

For more information see:

<http://www.justice.ie>, <http://www.orac.ie>

#### *An Garda Síochána*

In terms of organisational structure the Garda Information Technology Division, the Garda National Immigration Bureau (GNIB) and the Garda Technical Information Bureau (GTB) are all divisions of the Irish Police force, An Garda Síochána, under the overall control of the Garda Commissioner.

#### The Garda Technical Bureau

The Garda Technical Bureau is the longest established Specialist unit in An Garda Síochána. The Bureau comprises of 9 Sections each providing a specialist service to An Garda Síochána. They are as follows:

- Fingerprints.
- Ballistics.
- Photography.

- Mapping.
- Document Examination and Handwriting.
- Fogra Tora (Garda information booklet).
- Forensic Liaison Office.
- GCRO (Garda Criminal Records Office).
- Administration.

Within the various specialist sections, sub-sections have been established. They include:

- Photographic Digital Imaging.
- Shoe Mark and Tool Mark Identification.
- Fingerprint Chemical Development Unit.
- Ear prints.
- PRO-FIT (Facial Identification).
- Cheque Fraud.
- Serious Crime.
- Ballistics Data Reference Centre.

The Technical Bureau is headed by a Chief Superintendent (assisted by a Superintendent) who has responsibility for overall management of the Bureau, which has a personnel strength of approximately 200 Garda and civilian staff. The Chief Superintendent reports in turn to the Assistant Commissioner, National Support Services.

#### The Garda National Immigration Bureau

The Garda National Immigration Bureau (GNIB) came into operation in May 2000 and is responsible for all Garda operations pertaining to immigration matters in the State. A Detective Chief Superintendent with a Garda staff of 2 Superintendents, 3 Inspectors, 8 Sergeants and 55 Garda heads the GNIB. In addition, there are approximately 34 civilian support staff.

The Bureau became a necessity due to the exceptional increases in persons registering with the former Immigration and Registration Office and associated workload.

#### *The Garda Information Technology Division*

The Garda Information Technology Division is responsible for providing and maintaining leading I.T. support systems serving operational and specialist units within the Garda. A team of approximately 115 Garda and civilian staff, divided into 6 core teams, provides the following key capabilities:

- IT Security and Operations - Provides a 24 hour Service Desk; support services; hardware procurement; rollout of equipment, IT Security; investigation assistance.
- Research and Development - Research requests for new computer systems and technologies and ensure that the technologies chosen are the best and most appropriate solution to meet requirements of specialist sections.
- Project Co-ordination Office (PCO) - Deals with the co-ordination and project management between all the constituencies involved in the major projects, including IT, Telecommunications, Training College, external consultant's etc.
- Project Management Office (PMO) - Provides services to the various project teams, such as document libraries, storage of key documents and deliverables, etc.

- PULSE (Police Using Leading Systems Effectively) Project Teams - Responsible for the design, build and implementation of the PULSE system. PULSE is the largest IT system undertaken by An Garda Síochána and is one of the leading such police projects worldwide. Phase 1 of PULSE was deployed in 1999 and ensures accurate up-to-date information is available to all members in responding to the demands of a modern police force.
- Schengen Project Team - Responsible for the design, build and implementation of the Schengen Information System within An Garda Síochána.

## Fingerprint Project Background

An Garda Síochána is responsible for the management of all fingerprints taken under Irish law. The fingerprint records held by An Garda Síochána fall into two categories:

- All national fingerprint records.
- All national scenes of crime latent marks.

The Garda Fingerprint Bureau, a dedicated unit of the Garda Technical Information Bureau (GTB), is responsible for managing the National Fingerprint Identification System. It has operated the current Automated Fingerprint Identification/Recognition System (AFIS) since 1996 in conjunction with the Garda IT Centre. During this period of operation the Garda Fingerprint Bureau have developed considerable levels of expertise in the use and management of the AFIS system, as well as a reliance on the storage and searching power that such a computerised system provides.

The AFIS system is now due for replacement, or upgrade, for the following reasons:

- *Support lifecycles:* Support for the current AFIS system will expire in December 2006 and there is a need to move to a fully supported technical platform to underpin operations in the medium to long term.
- *Improved technologies:* A core capability of the AFIS system relates to crime solving and in particular latent matching. A new AFIS system should display 'best-of-breed' latent matching capability and be fully capable of leveraging all data within the repository (including palm-print data). In addition, the capability to utilise automated techniques for feature extraction/encoding, and latent marks captured at scenes of crime would enhance the latent capture and overall latent process.
- *Existing process enhancement:* In the case of ten-print and palm-print capture, more comprehensive use of Livescan techniques could be employed going forward, phasing out the reliance on manual capture processes. This serves to normalise the quality of data inputting the database and would assist in eliminating duplication of fingerprint capture among different organisations.
- *Extended user community:* Since the introduction of the original AFIS platform, the user community has grown and requirements have become more complex:
  - The advent of the Dublin Conventional and the introduction of the Eurodac system, together with the provisions of the Refugee Act 1996, requires the Office of the Refugee Applications Commissioner (ORAC) in Ireland to fingerprint asylum seekers and interface to the central Eurodac application. In addition, the ORAC process requires access to the Garda AFIS system for search, match and verification capability.
  - The establishment of the Garda National Immigration Bureau (GNIB), a division of An Garda Síochána, has further extended the AFIS user community, as potential capturers and searchers of relevant fingerprint databases. The introduction and storage of fingerprint biometric data on existing identification smart cards produced by GNIB is also planned as a future requirement.
  - GNIB requires the capability to search against both the Irish national fingerprint database (AFIS database) and international AFIS databases (e.g. Eurodac) in order to make determinations in relation to asylum applicants, illegal border crossings and resident non-nationals.
  - As the national fingerprint database is the sole repository of fingerprint information in Ireland both ORAC and GNIB require the ability to efficiently

upload and store fingerprint data to the national fingerprint database, for their own uses.

- *New process opportunities:* Based on the current requirements of the extended AFIS user-base, and the availability of new technologies within the fingerprinting and telecommunications fields, there are now considerable opportunities for new and more efficient processes:
  - Real-time processing of fingerprint queries in AFIS by leveraging more powerful match capability enabling faster verification.
  - Electronic capture and real-time query of fingerprints by An Garda Síochána and ORAC supporting new and more efficient decision processes within those organisations. In addition, the ability to capture and query of fingerprints by officers in the field using mobile search technology may allow for more timely decision-making and efficiency in processing.
  - Interconnection to external fingerprint databases (e.g. Eurodac).

### 3. Overview of Existing National Fingerprint Identification Systems

The GTB has operated the current AFIS system since January 1996. More recently they have provided a service to the ORAC for the searching, storage and verification of the fingerprints of asylum applicants.

- The AFIS system has a database of criminal ten-prints and unsolved scene of crime marks and a 'partitioned' database of asylum ten-prints managed on behalf of the ORAC.
- The current AFIS system does not cater for palm-prints. However the system has been altered to allow a certain level of palm-print matching to be carried out using the systems in place for fingerprints.
- Criminal ten-prints sent to the GTB are entered onto the AFIS; searched against both the criminal ten-prints and scene of crime databases. Fingerprint experts at the GTB verify all of the search results.
- Similarly, scene of crime marks sent to the GTB are entered onto the AFIS and searched against both the criminal ten-prints and scene of crime databases. Fingerprint experts verify all search results.
- Asylum Application ten-prints are regularly sent to the GTB and are entered and searched against the asylum ten-print database only. Fingerprint experts verify all positive hits and the results are then returned to the ORAC by courier.
- The majority of ten-prints sent to the bureau are manually generated following a standard ink-based process. However, three Livescan units, allowing for the digital capture of ten-prints are installed with one each at two Garda stations and one at Mountjoy Prison.

#### Existing AFIS Support Process Overview

At present the majority of both ten-prints/palm-prints and latents are processed manually into the AFIS, with the exception of ten-prints received via the Livescan units.

- The GTB operate a number of databases in conjunction with the AFIS system to track the status of all received fingerprint data. All received ten-prints are tracked in the **Correspondence Register** (This is a standalone database). It provides a snapshot view of all ten-prints received by the GTB.

Crime scene evidence is first processed via the chemical laboratory to recover latent mark data. This data is tracked via the **Exhibit Tracking System** (this is also a stand-alone database). It provides a snapshot view of all latents received by the GTB.

The AFIS system enables 3 key processes:

- *Quality Control:* the process of entering new fingerprint data into the AFIS; identifying, verifying and encoding the required characteristics.
- *Searches:* A range of searches against existing data (for example ten-print to ten-print, ten-print to latent, latent to latent, latent to ten-print).
- *Verification:* The process of verifying a match by a fingerprint expert. In the case where evidence of a match is needed for a court of law, 3 fingerprint experts must verify the match.

### **Installed AFIS Technical Overview**

The current Printrak 2000 AFIS system is made up of the following subsystems/workstations.

- One combination Data Storage and Retrieval/Minutiae Matcher Controller (DSR/MMC) including RAID for storage of fingerprint and palm-print images.
- One AFIS2000 Transaction Processor.
- Two Input Workstations (IS2000).
- Four Verification Stations (VS2000).
- Five latent Stations (LS2000).
- One Latent Case Station (LCS).
- Three Remote Livescans (LSS2000).

## Future Solution Overview

This section provides a high-level overview of the envisaged solution. It does not prescribe a solution, which will be the responsibility of the relevant bidders at the tender stage of this competition, but is meant to act as an explanatory guide to the main components of the future strategy.

### *Key components*

- *AFIS Client:* AFIS client(s) designed to capture fingerprint data and enable direct access to the AFIS Core capability (e.g. to upload ten-prints captured via a Livescan unit etc.) are envisaged. The AFIS client should support capability to integrate with existing external client software applications and supporting mid-tier processes.
- *AFIS Core:* The AFIS Core represents the main AFIS database and supporting functionality:
  - AFIS Functions: For example, matching, workflow, latent case management.
  - AFIS Database: Persistent repository of fingerprint data.
  - Viewing/Verification workstations: Dedicated workstations supplied with the AFIS Core supporting fingerprint processing and verification by fingerprint experts.
- *AFIS Enhanced Services:* Additional capability required to support the AFIS integration requirements with 3<sup>rd</sup> parties. For example, a match query that is required to interact with both Eurodac and AFIS Core would be handled in this layer. It is anticipated that these services will be composed of re-usable software components that leverage standard application server services such as transaction handling, message handling, web services exchange protocols, among others.
- *Security Services:* Providing role based secure, confidential, access to both internal and external users of the AFIS system
- *Management Services:* Providing administrative capability to AFIS end-users. For example, security and workflow management, performance management, alert and report generation.
- *Mobile Query Unit:* Providing the ability to do a two-finger search, from a mobile device with supporting finger scanner, against the AFIS database.
- *Secure Network:* The AFIS system will require the capability for the relevant agencies (e.g. ORAC, GNIB) to securely access AFIS functions located within the GTB.

### *Systems Integration*

A key component of this project will be the implementation of a robust, scalable, standards based integration framework to achieve the integration necessary with An Garda Síochána's existing systems. This integration framework must also allow for future integration needs within An Garda Síochána as well as supporting integration services to 'external' users or systems (e.g. other national government agencies or international AFIS systems). Summary information on the initial integration requirement is provided below.

#### *Integration with Existing Systems*

*Garda System (PULSE):* Since 1996, An Garda Síochána has been working on PULSE, an Information Technology and Change Management Project. This central system is the core



operational application designed to improve information gathering, collation and dissemination in An Garda Síochána.

- As PULSE is the core information base within An Garda Síochána it is a requirement that all new system developments must include integration with this information base where feasible.

**ORAC System:** ORAC is part of the Department of Justice, Equality and Law Reform and is responsible for handling all asylum applications in Ireland. It maintains a case management system for registering and processing all asylum applications. ORAC will need to extend their current manual fingerprint capture process to support the electronic capture, query and verification of fingerprints against Eurodac (specifically for the Dublin convention) and the AFIS database.

**GNIB System:** GNIB have responsibility for handling immigration at ports of entry, managing resident non-nationals and detecting illegal immigrants and failed asylum seekers within the country. The GNIB-information system (GNIB-IS) is extended to over 50 locations nationwide, including GNIB-HQ, District Headquarters, all ports of entry and the four main Garda Stations along the border with Northern Ireland that act as both registration and port of entry sites.

- The system functionality tracks the details of resident non-nationals who are granted leave to land or conditioned on entry to the country; those who have been refused leave to land in Ireland; and all resident non-nationals registered in the country. Resident non-nationals who claim political asylum at ports of entry are recorded as refusals that subsequently claim political asylum.
- All registered resident non-nationals are issued with a system-generated registration smart card. This card has the person's photograph and basic registration details on the front of the card as well as biographical and biometric data (facial data) stored on the microprocessor chip. The smart card enables verification of genuine cards, and more critically alerts immigration officers to forged cards. It is envisaged that fingerprint data could also be stored electronically on the smart card.
- An enhanced mobile solution of 20 rugged, handheld devices has been rolled out providing wireless access to information on the GNIB database at remote locations over the GPRS network, both inside and outside of Ireland. Two rugged laptops are also available to users.
- The AFIS system should support integration with existing GNIB-IS enabling the entering of a fingerprint record, search it against local, Eurodac, and possibly other international systems to obtain a result within a defined time period. This should be further extended to integrate the use of fingerprint storage on the registration smart card.

**Prison Service:** The prison service currently operates a Livescan unit to capture digital fingerprints. Any envisaged replacement to the existing Livescan capability should support and enhance existing capability to fully interact with the core AFIS system.

## 4. Preliminary Outline of Requirements

This section provides an outline of the requirements for a National Fingerprint Identification System (referred to in this section as the 'system') to meet the future needs of both the GTB and the organisations that will use its services.

- The system will support a fully-integrated and extensible solution that enhances existing processes and capabilities within the GTB:
  - Providing for the efficient capture of ten-prints, palm-prints and latents.
  - Providing for the upload of this data to the secure fingerprint repository.
  - Providing for the real-time verification of submitted queries.
  - Providing 'best-of-breed' latent processing and matching capability.
  - Providing the required service levels to the ORAC, GNIB, The Prison Service and general Garda operations in conjunction with the PULSE system.
- The system will support standards based connectivity to Eurodac and other external systems.
- The delivery of the system to support a National Fingerprint Identification System will encompass the following deliverables:
  - System design and development.
  - Database design and database implementation.
  - Migration of existing fingerprint data (ten-print, latent & palm-print), Correspondence Register etc. .
  - Software integration services.
  - Supply of integration software
  - Implementation services leading to the successful commissioning of the new system.
  - Training and user support services.
  - Process change management.
  - Project management.
  - Post-implementation support and maintenance services.
  - Supply, implementation and support of server hardware.
  - Supply, implementation and support of storage technology.
  - Services leading to the interoperability of the new hardware with current hardware platforms.
  - Installation, configuration and deployment of appropriate network and secure network access components.
  - Licences for the server operating system software running on any new equipment.
  - Licensing of appropriate application software.
  - Licensing of appropriate database software.
  - Long-term support of the overall solution as an option which must be provided and can be exercised at the sole discretion of An Garda Síochána.
- Where possible the system will leverage standard off-the-shelf hardware and software components.

- The system shall be modular enabling plug-in of different sub-systems.
- Where possible the system will support recognised open standards for application interaction (Services Oriented Architecture), security APIs (BioAPI) and data exchange (XML, NIST).
- Without prejudice, it is intended that the development of the system would commence in early 2005 with all key phases of the system implemented and deployed by December 2006.
  - The system will be built in phases, with detailed review, evaluation and refinement processes in each phase in order to facilitate an optimum solution.
  - It is anticipated that the phased delivery plan will account for the separate need to:
    - Replace and enhance existing operational AFIS functional capability and fingerprints repository.
    - Provide new real-time electronic capability to external agencies, and integrating with their existing software systems where required.
- The supplier will demonstrate capability to provide long-term support to the system, post deployment.

#### **Outline Garda Technical Bureau AFIS Requirements**

- The system will demonstrate efficiency and effectiveness in terms of timeliness of results, improved processes and reduction of duplication of effort.
- The system will be able to store, retrieve, and compare ten-prints, latents and palm-prints (including writer's palm).
- The system will demonstrate advanced capability in real-time search and verification of ten-prints.
- The system will demonstrate advanced capability in latent processing (supporting 1000dpi) and matching.
- The system will provide automated and configurable workflow capability.
- The system will provide latent case management.
- The system will support performance management.
- The system will support fault tolerant and disaster recovery capability.
- The system will support web-based interfaces.
- The system will support secure external access.

#### **Searches**

- The system will support initiation of searches from the point of capture.
- The system will support results of AFIS database ten-finger fingerprint searches within set timeframes at point of capture.
- The system will support results of database fingerprint searches against Eurodac and other external systems.
- The system will support remote interfaces and/or interconnections to existing facilities to allow the direct entry and searching of ten-prints as outlined for the ORAC and GNIB.
- The system will support use of various input types (finger, ten, palm-prints) in searches against all sections of the database.
- The system will be able to obtain fast response times and high accuracy for ten-prints of all types without the need for initial quality control.

- The system shall be able to configure and utilise different fingerprint encoding and matching sub-systems.

#### **Database**

- The system will demonstrate reliable and performant data storage.
- The system will store and use information in a timely manner, with the capability to insert into the database all fingerprint records (ten-print, palm-print, latents) captured.
- The system will support multiple print categories, for example:
  - Ten-prints of criminals.
  - Criminal scene of crime marks.
  - Criminal palm-prints.
  - Ten-prints of all asylum seekers.
  - Ten-prints of all illegal immigrants.
  - Ten-prints of resident non-nationals.
- The system will maintain a high quality database through quality control for immigration prints and criminal activity for poor quality fingerprints.
- The system will support an extensive back record conversion (BRC) and full migration of all existing ten-finger, palm and scene of crime marks (ensuring this invaluable existing repository is fully available to all future database searches at 'go-live' of AFIS core system).

#### **Print Capture**

- The system will utilise modern Livescan units for the electronic capture of prints.
- The system will integrate with external systems, such as GNIB, ORAC and PULSE.
- The system will integrate a Livescan capture process within existing external client applications.

#### **Latent handling**

- The system will demonstrate high performance for criminal identification in terms of accuracy of results (possibly using desk based expert workstations) and the ability to upgrade performance going forward.
- The system will provide facilities to centrally manage the criminal fingerprint entry and search requirements.
- The system will support separate matching algorithms for latents and ten-prints.
- The system will provide facilities to centrally enter and store palm-prints.
- The system will provide facilities to centrally enter and search scene of crime palm marks.
- The system will provide for the high quality digital capture of latent marks at the scene of investigations.

#### **Network**

- The system will support network and transaction security through standard practices such as encryption, private secure networks (VPNs, firewalls/routers/DNS servers/intrusion detection) and security policies.

#### **GNIB Outline Requirements**

- Fingerprints of asylum applicants and illegal entrants intercepted at Port of Entry or other locations to be captured using Livescan devices or other means and submitted electronically to the system, for searching against the National AFIS; and possibly Eurodac and other external databases to be determined.
- Ability to receive, from the system, results of asylum applicant and illegal entrant searches back to the Port within a set timeframe. This includes the ability for the system to do a real-time search both against AFIS database, and to enable a real-time verification by a fingerprint expert in the event of a "hit".
- Asylum seekers granted leave to land are given a documentation pack and asked to attend ORAC offices. Once presenting at ORAC it should be possible for ORAC to electronically retrieve the fingerprint data taken at port-of-entry from Irish AFIS, Eurodac and other external systems.
- The ability for the system to provide an, 'out of hours', unverified response to enable the possible detention of a person pending a confirmed result.
- The ability for the system to capture fingerprints of registered non-nationals (i.e. existing holders of registration cards) onto the AFIS system at their re-registration date, or if not registered, at point of first registration.
- The ability for the system to do a real-time search against the AFIS database at point of registration to eliminate duplicate registration.
- The ability for the system to capture a fingerprint at non-national registration onto the registration smart card. The system should support the ability to do a verification search against the AFIS database on re-registration to validate identity.
- The ability for the system to verify the identity of individuals 'in the field' in real-time on a mobile device, based on the capture of two-prints and to perform a search against the national and international AFIS systems (e.g. Eurodac).

#### **ORAC Outline Requirements**

- The ability for the system to quickly and easily check in real-time the existence of asylum applicant fingerprint records on both the Irish and external AFIS systems (e.g. Eurodac) without the need, as currently, for duplicate fingerprint queries into the FIT/NAP-Eurodac and National AFIS databases.
- The ability for the system to provide Livescan entry of fingerprints, replacing the current manual fingerprint process.
- The ability for the system to print fingerprint records captured by Livescan onto fingerprint forms (for hard copy storage) at the ORAC and/or the GTB.

#### **General Requirements**

The supplier will be expected to:

- Utilise a system development standard methodology.
- Have comprehensive quality assurance procedures in place.
- Conform to the PRINCE II project management methodology.
- Provide training to a number of different teams within An Garda Síochána, ORAC and the Prison Service.
- Locate implementation teams in Ireland.
- Provide post implementation support for a period 2 to 5 years after the go live date, as an option, which must be provided by the supplier and to be exercised at the sole discretion of An Garda Síochána.

### Standards Compliance

The system will support the following standards:

- EURODAC standard in full.
- NIST standards compliant record interchange format of fingerprint records and related transactions including images, demographic data and photo images interchanged between differing AFIS systems.

Where appropriate the system should indicate compliance with the latest IT and AFIS standards as defined by the FBI, ANSI/NIST, Eurodac, and INTERPOL including the following image capture quality, image compression, print quality, data interchange standards:

- ANSI/NIST-ITL (INTERPOL) 1-2000 (version 4.22) data format for the interchange of fingerprints.
- ANSI INCITS 377 (pattern based data interchange format).
- ANSI INCITS 378 (minutiae based data interchange format).
- Common Biometric Exchange File Format (CBEFF) data structures.
- FBI Implementation for Fingerprints.
- FBI IQS scanning acquisition.
- WSQ data format compression.
- XML Data Interchange.

The system will comply with relevant IT equipment standards.

The system will comply with relevant health and safety standards.

## 5. Procurement Process

- 5.1 This competition is being conducted under the "restricted procedure" rules governing public procurement in operation within EU member states. The award of contract will involve two competitive stages. This is the first stage of the competition, which constitutes a pre-selection process; the second stage will be a tender competition confined to the parties pre-selected from the first stage. This briefing document relates to the first stage only. An Invitation to Tender (ITT) detailing the solution requirements will be issued to the parties selected on foot of the first process.
- 5.2 It is envisaged that between 5 and 8 service providers will be selected from the suppliers and invited to tender, provided there is a sufficient numbers of suitable suppliers. The awarding authority seeks to award a single contract, to a single primary supplier, for the procurement of all goods and services associated with this supply. The primary supplier will be the single responsible point of contact for the contract delivery. Interested parties are at liberty to make their own arrangements regarding formation of groups/consortia. The contracting authority will play no role in facilitating this.
- 5.3 The awarding authority for this procurement is the Department of Justice, Equality and Law Reform with An Garda Síochána.

## 6. Administrative Arrangements

- 6.1 Six copies of each application for pre-selection must be provided, in paper format and, a 'soft copy' on CD (in both Microsoft® Word 2000 & Adobe® PDF formats), in a sealed envelope marked 'National Fingerprint Identification System – Briefing Document' and addressed to:
- Director of Finance,  
Tender Reception Office,  
An Garda Síochána,  
Garda Headquarters,  
Phoenix Park,  
Dublin 8,  
Ireland.
- 6.2 Under no circumstances will applications by fax, electronic mail or by any other electronic format be accepted.
- 6.3 The applications must be delivered to reach the above address not later than **3pm, February 4<sup>th</sup>, 2005**. Under no circumstances will applications be accepted after this time. Applicants are requested to make their own arrangements to obtain proof of delivery by, for example, obtaining a receipt.
- 6.4 Any queries should be addressed, by e-mail, to [fintan.fanning@garda.ie](mailto:fintan.fanning@garda.ie).



## 7. Notices and Conditions

- 7.1 Detailed contractual arrangements are beyond the scope of this document. However, the following conditions apply to the competition and should be noted, and where appropriate, responded to in the applicant's document.
- 7.2 The awarding authority undertakes to hold confidential any information provided by suppliers in their response documents, subject to its obligations under law, including the Freedom of Information Acts 1997 and 2003.

Note that under the Freedom of Information Acts, information provided by you may be liable to be disclosed where the public interest value of releasing such information is deemed to outweigh the right to confidentiality. An Garda Síochána will consult with the party supplying confidential information before making any decision on releasing such information in response to a request under the Acts.

You are asked to consider if any of the information supplied by you in your response document should not be disclosed because of its sensitivity. If this is the case, you should when providing the information, identify same and specify the reasons for its sensitivity. If you do not identify it as sensitive and An Garda Síochána, on consideration, do not deem it sensitive then it is liable to be released in response to a Freedom of Information Act request without further consultation with you. An Garda Síochána will consult with you about sensitive information before making a decision on a request that it receives pursuant to the Freedom of Information Acts.

If you consider that none of the information supplied by you is sensitive please make a statement to that effect. Such information is liable to be released in response to a Freedom of Information Act request.

- 7.3 Before contracts are awarded, the successful supplier (and agent, where appropriate) will be required to comply with the prevailing tax clearance procedures viz.: A successful supplier resident in Ireland will be required to promptly produce a Tax Clearance Certificate from the Irish Revenue Commissioners. A successful non-resident supplier or sub-supplier will be required to produce a statement (in lieu of a Tax Clearance Certificate) from the Irish Revenue Commissioners confirming suitability on tax grounds to be awarded the contract. Application for either of the above may be made to the Irish Revenue Commissioners by way of a standard form, *which will be provided to the successful supplier(s) by the Garda IT Department in due course*. Where a certificate or statement expires during the course of the contract, the Department will require a renewed certificate or statement. All payments under the contract will be conditional on suppliers being in possession of valid certificates at all times.

**In responding to this document, applicants for pre-selection should state that their tax affairs are in order and that obtaining a Tax Clearance Certificate or Statement of Suitability from the Irish Revenue Commissioners will not pose a problem for them.**

- 7.4 The awarding authority will not be liable for any costs incurred by respondents in the preparation, submission or presentation of applications or tenders, or any associated work or effort howsoever incurred.
- 7.5 Whereas this briefing document is issued in good faith, no legitimate expectation shall arise therefrom and the Department shall not be obliged to award a contract or proceed to further stages in the procurement process.
- 7.6 Any contract concluded under this procurement will be governed by Irish law and, subject to arbitration provisions, the parties will submit to the exclusive jurisdiction of the Irish Courts.

- 7.7 As provided by Article 11.3(f) of EU Council Directive 92/50/EEC, the awarding authority reserves the right to adopt the negotiated procedure to engage the successful supplier from this procurement to undertake new services consisting in the repetition of similar services which conform to this basic project, in accordance with the said Article.
- 7.8 Any conflicts of interest involving a supplier (or suppliers, in the event of a group or consortium application) must be fully disclosed to An Garda Síochána, particularly where there is a conflict of interest in relation to any recommendations or proposals put forward by the supplier.
- 7.9 Any "registerable interest" involving the supplier or suppliers and An Garda Síochána, the Minister for Justice, Equality and Law Reform, members of the Government, members of the Oireachtas (Irish Parliament) or employees of the Department of Justice, Equality and Law Reform or their relatives must be fully disclosed in the application or should be communicated to the Department of Justice, Equality and Law Reform immediately upon such information becoming known to the supplier, in the event of this information only coming to their notice after the submission of an application. The terms "registerable interest" and "relative" shall be interpreted as per Section 2 of the Ethics in Public Office Act, 1994.
- 7.10 An Garda Síochána will require the successful Supplier to sign a non-disclosure agreement on entering the second stage. Suppliers should acknowledge their acceptance of this condition.
- 7.11 Work in relation to this project will be undertaken on-site, in An Garda Síochána's various premises in Ireland and in ORAC.
- 7.12 All personnel assigned to work on this project must satisfy the security clearance procedures of An Garda Síochána prior to commencement of work. Suppliers should acknowledge their acceptance of this condition.

## 8. Material Required in Response Document

An Garda Síochána will rate and rank potential service providers (suppliers) only in accordance with the information supplied in response to the qualification criteria set out below. The application for pre-qualification in respect of this contract must be in a format specified hereunder. Failure to do so may result in rejection of the application. An Garda Síochána reserves the right to seek clarification of any information submitted.

Response material required

### *Response Section A: General Information*

- 8.1 The application must include the name, address, telephone and fax number of the supplier and the name and e-mail address of the contact person.
- 8.2 Where a particular application is based on a group/consortium of business interests, the document must identify:
  - a) The prime partner in the group/consortium.
  - b) The number of parties involved and names of each, and
  - c) The proposed arrangements for its operation, i.e. the area of participation of each party in the context of the project.
  - d) Confirmation that the prime partner will be the sole contracting authority.
- 8.3 Suppliers must provide a statement to the effect that none of the excluding circumstances as outlined in Article 45.2 (a) – (g) inclusive of Directive 2004/18/EC applies to them (Appendix A refers).
- 8.4 Confirmation of acceptance and agreement with each condition set out in Section 7 of this Briefing Document.
- 8.5 Where the supplier is a group or a consortium, or where it is proposed to sublet any portion of the contract, the information above must be provided in respect of each firm forming part of the group or consortium.

### *Response Section B: Suppliers Financial and Economic Standing*

- 8.6 Suppliers are required to give a brief history of each member of the bidding consortium outlining their line of business and any areas of specialisation.
- 8.7 Details of the supplier's company structure, or each member of the bidding consortium where relevant. If the bidding entity is a subsidiary company, details of the parent company must also be submitted where the parent company is to be relied upon as part of this project.
- 8.8 The nature of the relationship between the parent and subsidiary companies must be set out especially in terms of the financial or contractual guarantees between the parent and subsidiary.
- 8.9 Suppliers must provide the following information relating to their financial and economic standing:
  - o Evidence of relevant professional risk indemnity insurance.
  - o A statement of the supplier's overall turnover and its turnover in respect of the specific services which would be relevant to this contract (see Section 4 of this document for a preliminary outline of the services contemplated for this contract), for each of the *three* previous financial years.
  - o Audited Annual accounts for each of the previous three financial years.

- 8.10 Statements from bankers indicating the minimum level of working capital capacity of the firm, which would be available to fund the project.
- 8.11 Suppliers are required to list all the contracts over the past 5 years that resulted in litigation or arbitration proceedings, with an indication of the amounts in dispute and the resolution of the dispute.
- 8.12 Suppliers are required to state their willingness to post a performance bond up to 25% of the value of the final contract.
- 8.13 As provided by Article 47.5 of Directive 2004/18/EC, if for any valid reason the supplier is unable to provide the information requested above, they may prove their economic and financial standing by production of any other document, which An Garda Síochána considers appropriate.

*Where the supplier is a group or a consortium, or where it is proposed to sublet any portion of the contract, the information requested under this heading must be provided in respect of each firm forming part of the group or consortium.*

### ***Response Section C: Suppliers Technical Capability***

Suppliers must provide the following information relating to their technical capability:

- 8.14 Please see Section 4 of this document for a preliminary outline of the services contemplated for this contract. In particular, please ensure that your application addresses your approach to meeting **all of the requirements listed**. Suppliers are requested to provide a description of the technologies used in their solutions and describe how these were implemented in environments with similar requirements.
- 8.15 Provide an overview of the business strategy stating specifically the commitment to development, implementation and support services that are required here in relation to package and bespoke elements of the solution.
- 8.16 Details of the supplier's **relevant professional qualifications and expertise**. In particular, please provide details of the members of the overall team who would be responsible for providing the services.
- 8.17 A statement of the supplier's average annual manpower and the number of managerial staff employed per annum, for each of the last three years.
- 8.18 A list of similar contracts undertaken by the supplier. For each project, please provide:
  - o A description of the work undertaken.
  - o Details of the value and duration of the projects, and
  - o Details of the parties for whom the work was undertaken.
- 8.19 Full contact details for relevant reference sites where the supplier or consortium has implemented similar solutions. Site visits/calls may be arranged as part of the short-listing process.
- 8.20 Details of the technical facilities, relevant to the assignment, which would be available to the supplier.
- 8.21 Details of ability to deploy and support the project team in Ireland.
- 8.22 A description of the supplier's measures for ensuring quality, which would be relevant to the contract. Where use of formal quality standards is envisaged and/or where the respondent has obtained formal quality assurance accreditation, details of same should be provided by reference to the appropriate standards.

- 8.23 Where the supplier is a group or a consortium, or where it is proposed to sublet any portion of the contract the response must show the parties experience of working together in providing similar solutions.

*Where the supplier is a group or a consortium, or where it is proposed to sublet any portion of the contract, the information requested under this heading must be provided in respect of each firm forming part of the group or consortium.*

### **Evaluation Criteria**

It is envisaged that between 5 and 8 service providers will be selected and invited to tender, provided there is a sufficient numbers of suitable suppliers, based on the following criteria:

- Completeness of response and adherence to the required format.
- Response to mandatory requirements and acceptance of response conditions (Section 7).
- Supplier's financial and economic information.
- Supplier's technical capability.

## Appendix A

Extract from Article 45 of Directive 2004/18/EC of the European Parliament and of the Council of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts.

### *Article 45*

Personal situation of the candidate or tenderer.

2. Any economic operator may be excluded from participation in a contract where that economic operator:
  - (a) Is bankrupt or is being wound up, where his affairs are being administered by the court, where he has entered into an arrangement with creditors, where he has suspended business activities or is in any analogous situation arising from a similar procedure under national laws and regulations.
  - (b) Is the subject of proceedings for a declaration of bankruptcy, for an order for compulsory winding up or administration by the court or of an arrangement with creditors or of any other similar proceedings under national laws and regulations.
  - (c) Has been convicted by a judgment which has the force of res judicata in accordance with the legal provisions of the country of any offence concerning his professional conduct.
  - (d) Has been guilty of grave professional misconduct proven by any means which the contracting authorities can demonstrate.
  - (e) Has not fulfilled obligations relating to the payment of social security contributions in accordance with the legal provisions of the country in which he is established or with those of the country of the contracting authority.
  - (f) Has not fulfilled obligations relating to the payment of taxes in accordance with the legal provisions of the country in which he is established or with those of the country of the contracting authority.
  - (g) Is guilty of serious misrepresentation in supplying the information required under this Section or has not supplied such information.

END