National Headquarters/ Logistics Support Division
Procurement and Sales Department
Technology Procurement Section
Phone number: 08-9124130

27.3.2025

re: Preliminary Request for Information (RFI/ RFD) - number 2025/6

Request for information, demonstration, and presentation of capabilities on the subject of:

AFIS (Automated Fingerprint Identification System)

1. General

1.1. The Israel Police/Division of Identification and Forensic Sciences interested in receiving information about an automated criminal AFIS system (systems intended for police departments and law-enforcement agencies), for identifying, comparing and storing fingerprints and palm prints (automated fingerprint identification system) (hereinafter "AFIS"), and to have a demonstration thereof, as necessary.

1.2. The Israel Police wishes to remain at the forefront of the most advanced systems worldwide for criminal fingerprint management and to use qualitative and innovative capabilities, according to its needs. The Israel Police therefore seeks to examine the latest AFIS technologies worldwide (hardware and software), and to adapt them to its needs. It is hereby clarified that this request for information refers to AFIS systems with fingerprint and palm print capabilities. Wherever "fingerprints" are mentioned in this RFI, palm print capabilities are intended as well.

1.3. Participants interested in responding to this request are required to provide as much relevant information as possible regarding the product/service or its alternative, including the extent to which the product/service meets the needs specified in this document.

1.4. The RFI process is not a tender process and should not be construed as a process to select the participant's product/ service or as a request for proposals. Furthermore, this RFI should not be construed as a commitment of any kind on the part of the Israel Police towards the participants to publish a tender or to undertake any follow-on activities pursuant to this process, including an RFD and future procurement. This RFI does not create any

contractual obligation between the Israel Police and the respondent to the RFI. Following receipt of the responses to this RFI, the Israel Police will consider any follow-on activity at its sole discretion.

1.5. Should the Israel Police decide on proceedings to hold demonstrations (RFD), the request will be made to participants whose responses to the RFI met the need defined in section 5.8.1, subject to the decision and approval of the Tenders Committee.

1.6. It is hereby clarified that any contractual engagement of the Israel Police is subject to the Mandatory Tenders Law, and that the RFI process will not make the tender process redundant in accordance with the Mandatory Tenders Law, should the Israel Police decide to initiate one. Participation in the current process should not be construed as prerequisite or obligation for participating in a future tender, should one be published. In addition, nothing in the response or in the content of the response to this request confers any advantage or disadvantage whatsoever to the participants in this process .

1.7. Should the Israel Police decide to purchase a product/ service, the purchase shall be in accordance with a particular specification, which may differ from the requirements in this document.

1.8. All the expenses incurred in the response to this request are the sole responsibility of the participants and at their expense, including supplementing of additional information, and holding of meetings and discussions on the subject, etc. It is emphasized that the participants will not be entitled to any compensation or indemnification in respect of expenses and/or damages as shall be caused them in respect of their response to the request, including in respect of a presentation and/or demonstration, if any.

1.9. Subject to that stated in section 1.10 below, and after examining the information, the Israel Police will be entitled to use the information that it receives from the participants as it sees fit, including for the purposes of examining the possibility of entry into a contractual engagement on the subject and of formulating the requirements for such contractual engagements, in order to write a specification and tender or any other document, and in order to compile a list of potential suppliers.

1.10. Subject to any law, the Israel Police shall keep confidential the information that it receives within the framework of the response, and will not make use thereof, as specified below:

1.10.1. The information shall not be published publicly.

1.11. The intellectual property rights of the respondent shall not be infringed**.** The information shall not be used for commercial purposes, except for the purposes stated in this request.**1.10.4.** The information shall not be shared with third parties, except with entities involved in the engagement process, such as professional advisors.

1.12. Notwithstanding what is stated in section 1.10 above, the Israel Police will be entitled to approach the respondent and ask to use the information, in the manner mentioned in sections 1.10.1 to 1.10.4 above.

1.13. Due to various constraints, it is possible that these proceedings will be canceled, or reduced in scope or postponed. The Israel Police will not incur any expense or payment in respect of postponement or cancellation or reduction in the scope of the proceedings or in respect of any other decision on the part of the Israel Police with respect to the proceedings.

1.14. The Israel Police will be entitled to extend and/or postpone the deadlines specified in this document, at its sole discretion.

1.15. The Israel Police reserves the right to hold clarification meetings with the participant, at its sole discretion.

1.16. A participant that submits a response to this request declares that:

1.16.1. It agrees to all that specified the document and undertakes that the respondent shall not have any claims and/or demands against the Israel Police or against any other entity with regard to use of the information that it shall provide.

1.16.2. There is nothing in the information submitted by the participant or in its future use to infringe upon the rights of a third party, including copyrights, and that it alone will be liable for any demand or claim arising from an allegation that the rights of a third party as aforesaid were violated in the context of the use of the information submitted, and it will compensate the Israel Police immediately upon receipt of the demand for any amount that may be demanded and/or claimed for payment as a result of a claim or demand as aforesaid, including expenses and attorney's fees.

1.16.3. The documents in this request are the exclusive property of the Israel Police.

1.17. Do not make the response contingent on any conditions whatsoever.

1.18. This request will be published after the approval of the Israel Police Tenders Committee, and under its supervision.

2. Description of the existing system

2.1. **The Israel Police has a criminal AFIS system CAFIS Version 6, which** has been customized to meet the specific needs of the Israel Police and is maintained by Thales company. The system has been operesional since January 2014.

Its deployment was completed and declared fully operational in January 2016.

2.2. **The purpose of the system**:

To perform all system-wide FP- and PP-related tasks (acquisition, processing, storage, retrieval, comparison, verification, and identification) concerning suspects and unsolved crime scene latents, and other identification data such as mug-shots, demographic data, etc.
To enhance INP ability to process evidence, and to apprehend and prosecute suspects.

2.3. **The goals and Targets**

2.3.1. To manage the fingerprinting in several repositories.

2.3.2. To enroll, process, store, retrieve and manage the ten prints of a person, from different sources.

2.3.3. To enroll, process, store, retrieve and manage the latent fingerprints from latent prints, from different sources.

2.3.4. To identify suspects and link them to prints from crime scenes (latent prints), while the suspect is being held by the police, in real time.

2.3.5. To enroll, store and manage images and demographic and physical data, as metadata, alongside the fingerprints.

2.3.6. To identify bodies and disaster victims.

2.3.7. To authenticate/ identify persons on the basis of fingerprints.

2.3.8. To authenticate/ identify persons who carry a biometric ID card by biometric matching with the ID card data.

2.3.9. To interface to internal systems within the Israel Police, as well as to systems external to the Israel Police, such as the systems of the FBI, INTERPOL, the Ministry of Interior, etc.

2.4. **Below is a breakdown of the existing end-point stations at the Israel Police**:

2.4.1. Admin Stations.

2.4.2. Full Work Station for Expert.

2.4.3. Live Scan stations - electro-optic live scanning of fingerprints.

2.4.4. Remote Scan stations - for scanning latent prints and inked prints.

2.4.5. Victim Stations - for identifying dead victims.

2.4.6. Portable Work Station Expert - remote expert stations that enable mobile work from anywhere in the world, both online against a central repository and off-line against a local repository.

2.4.7. Portable Live Scan stations - remote live Scan fingerprinting stations that enable mobile work from anywhere in the world, both online against a central repository and off-line against a local repository.

2.4.8. Fingerprint scanners at investigator stations to authenticate/ identify an identity (Fast ID), operated from the Israel Police systems. The scanners include a built-in smartcard reader.

2.4.9. Fingerprint scanners for patrol car, operated from Israel Police systems, in order to authenticate/ identify an identity.

2.4.10. Mobile device - a portable terminal for fast ID.

2.4.11. Fusion Mobile Device - a portable terminal for scanning and identifying latent prints at the scene of a crime in real time.

3. The RFI process

3.1. The participants shall transfer information about the product(s)/ service(s) on their behalf to the Israel Police. The information shall include maximum details and documents.

3.2. **The following documents, at the very least, must be attached to the response (documents can be submitted in the English language)**:

3.2.1. The specification for the system that is the subject of this response, and any other documents containing detail of the system's capabilities.

3.2.2. Certificate of compliance with standards for criminal AFIS fingerprint systems, which the system that is the subject of this response complies with.

3.2.3. The results of the accuracy audits for the system that is the subject of this response, conducted by one or more of the international standards organizations (such as the FBI, NIST/ANSI) in the past 3 years.

3.2.4. Certificate of compliance with information security and cybersecurity standards, such as: NIST, ISO, SOC2, GDPR.

3.3. **Information about the system manufacturer's experience that is the subject of this response and its users**:

3.3.1. Manufacturer's experience: the manufacturer's experience in developing and maintaining an AFIS, including number of years of experience, details about systems, and the size of the customer base.

Shall be completed in the table enclosed as **Annex A**.

3.3.2. Details about customers (with emphasis on security bodies in the member states of the European Union, the United States, Canada, Australia and New Zealand) at which a criminal AFIS is installed and maintained, containing a repository of more than 4,000,000 fingerprint records.

This shall be completed in the table enclosed as **Annex B**.

3.4. **Information about the system's capabilities** (will be completed in Annex C):

3.4.1. **General description of the system, technical (hardware and software) and functional review, with emphasis on the following capabilities**:

3.4.1.1. Possible sources of enrollment and input of ten prints (live scan stations, scanning of prints, external media, interfaces, crime scenes, etc.).

3.4.1.2. Possible sources of input of latent fingerprints (scanning of latent prints, external media, interfaces, crime scenes, etc.).

3.4.1.3. Authenticating/ identifying a person or latent prints, on the basis of fingerprints from different sources (interfaces, mobile/ cellular devices, etc.), against a database, with emphasis on the following functions:

- TP-TP function.

- TP-UL function.
- LT-TP function.
- PL-TP function.
- LT-UL function.
- PP-ULP function.
- LP-ULP function.
- Coding from within an image function.
- Ability to define a closed group and to perform a search against this group only (Close search), using the function: LT-TP, LP-PP, LP-ULP, TP-TP, LT-UL, TP-UL.

3.4.1.4. Details of performance, response times, system's level of accuracy as a function of the search servers, their processing capacity and the quality and accuracy of the algorithm.

3.4.1.5. Details about the ability of the system to integrate with external systems, including protocols supported, such as SDK and API. The company shall provide details about its experience in implementing interfaces to the systems of international law enforcement agencies.

3.4.1.6. Coding of finger and palm prints of a person from a photograph taken with a camera.

3.4.1.7. Documenting and recording of fingerprints on the scene (prints and latent prints), using a mobile device, and sending them to the central system from different sources.

3.4.1.8. Taking photographs of people's faces and storing the images as part of the Metadata; advanced image processing capabilities.

3.4.1.9. Details of the functions for processing, matching, analyzing and updating fingerprints and latent prints, by an expert.

3.4.1.10. Details of performance of the work process by a second expert on the screen, using ACE-V charting, and processing of the information, in order to present it in a court of law.

3.4.1.11. **Generation of queries and reports** - details of all the possibilities available for generating various reports in the system, including details of these capabilities using artificial intelligence (AI).

3.4.1.12. **System administration** - details of the system admin station capabilities also addresses the ability to define profiles and different privileges for different users.

3.4.1.13. **Training and integration** - details of the means of training and practicing on the system (stations, hardware and software), for the different stations and different operators.

3.4.1.14. **Test environment** - the company shall present the solution proposed for setting up a system test environment.

3.4.2. **End-point stations**

3.4.2.1. The participant shall provide information about the hardware and software solutions for the end-point stations specified in section 2.4 above, and for additional end-point stations, if any, with respect to the system that is the subject of the response, with emphasis on the following topics:

- Technical specification for the computer. Is the application supported by standard computer stations?
- Operating system supported. Is the station supported in a Microsoft environment, and in the various versions of Microsoft's operating systems?
- Types of fingerprint scanners, including standards supported, with emphasis on an FBI standard.
- Biometric camera (resolution and standards supported).
- AI capabilities.
- Support for off-line mode.
- Biometric data encryption capabilities in the station.
- Control of user logins and privileges.
- How software updates are distributed.

3.4.2.2. **Mobile devices - fingerprint scanners and portable terminals**

Fast ID device designed to authenticate or identify a person:

- Details about the live scan surface, with emphasis on the physical size of the device, the size of the surface and the resolution.
- The participant shall describe the device's technical data and whether it includes a standard API for developing interfaces and an SDK for development work.
- The manner of the connection (standard USB, type c) for the end-point unit, such as a computer, tablet.
- The operating systems supported by the device (Windows, android, etc.).
- Does the device support CITRIX (Citrix) Terminal Server?

3.4.2.3. **Portable terminal/ tablet for Fast ID**

The participant shall describe the device, with emphasis on the following functions:

- Checking against a local repository (Wanted List), as well as against a central database via the Israel Police's internal communications and via cellular communication.
- Does the portable terminal include a contact/ contactless smart card reader?
- The operating system supported by the portable terminal.
- The types of the connections on the portable terminal.
- The level of impermeability to moisture and dust.
- Ability to withstand high temperatures.
- Details of the battery's capabilities.

3.4.2.4. **Mobile station to enroll fingerprints from bodies**

- Details of the mobile system, which will be able to take fingerprints directly from bodies and identify the prints against a mobile repository and against the central database.
- Including all the components needed to perform all the actions required to enroll fingerprints from bodies.

3.4.2.5. **A mobile device to photograph fingerprints at the scene of a crime**

- Details of the capabilities of the mobile device that the various crime scene investigators will use to photograph fingerprints from the crime scene and to transmit that to the central system via cellular communications in order to search the repository.

3.4.3. **Data migration**

3.4.3.1. Description of the data migration capabilities and of the migration process from an existing system to the system that is the subject of this response, with emphasis on the following repositories:

3.4.3.1.1. Repository of fingerprints and palm prints from different sources, that were processed during their entry into and saving in the system.

3.4.3.1.2. Database of latent finger and palm prints that underwent processing during their entry into and saving in the system.

3.4.3.2. Database cleansing capabilities during the migration.

3.4.3.3. Ability to use AI in the data migration process.

3.4.3.4. The preparations required of the supplier of the system being migrated for purposes of the migration.

3.4.3.5. The company shall specify its experience in migrating the data of a system containing at least 3,000,000 ten prints and 250,000 latent fingerprints, with emphasis on the following parameters:

3.4.3.5.1. Details of the customers and the customers' contact persons (in the event of mandatory confidentiality, provide details on the type of customer and general information).

3.4.3.5.2. The manufacturer of the system from which the data were migrated.

3.4.3.5.3. Type of database

3.4.3.5.4. How long it took to perform the migration.

3.4.3.5.5. The manner of the transition from the old system to the new one, including reference to functional continuity.

3.4.4. **Information security and cybersecurity**

Description of the characteristics of the service and the system regarding information security and cybersecurity issues, with emphasis on the following parameters:

3.4.4.1. Details of information security and cybersecurity standards that the organization and the system are compliant with, such as NIST, ISO, SOC2, GDPR, etc.

3.4.4.2. Information security and cybersecurity controls in use in the system/ service.

3.4.4.3. Manner of integration of the SDLC process in the lifecycle of the system/ service, including software testing.

3.4.4.4. If the participant proposes using the IT infrastructure of another supplier, it must state this and attach a document describing how the responsibility is divided between it and the additional infrastructure supplier, and what measures it takes to protect the data from vulnerability at the infrastructure level.

3.4.4.5. Details of the implementation and manner of support for the monitoring and control systems, for the transfer of log and events files to automation and security monitoring systems, such as SIEM and SOAR, e.g. SYSLOG.

3.4.4.6. Details of the system's support for authentication mechanisms such as SSO and IAM.

3.4.4.7. Details as to whether the system includes the possibility of a biometric check for authorization to log in to the system.

3.4.4.8. Details about the system's support for imposing a password changing policy that includes defining of variables such as: length, complexity, expiration time, history, MFA enforcement, etc.

3.4.4.9. Details of how the system supports Least Privilege access for users for the actions they are allowed to perform in the system, in order to protect

the data against unauthorized access, exposure, tampering, modification or deletion.

3.4.4.10. Details of all the encryption protocols that exist in the system (including type of encryption, such as AES 256 bit, and key size, such as 2048 bits or greater), for end-to-end data encryption, and data encryption both in transit and at rest.

3.4.4.11. Details of the system support for storing encryption keys in hardware security modules (HSM) and key management services (KMS) and/or any other solution for securing keys. The Company shall specify how this response is implemented.

The Company shall specify any additional information about information security and cybersecurity relating to the system.

3.4.5. **The system infrastructures**

3.4.5.1. Information about the hardware requirements, the operating system and network infrastructures required.

3.4.5.2. The communications solution for operation in an ACTIVE-ACTIVE configuration, including definition of traffic files required between the sites.

3.4.5.3. The volume and data transfer rate of the files and the minimum bandwidth that enables normal operation. Note that the company will be required to work on the basis of the active infrastructure that exists at the Israel Police.

3.4.5.4. The company shall specify the manner of the response - web solution/ installation of local software (client) / CITRIX.

3.4.5.5. Situation in which communication between the core and the end-point station is disconnected.

3.4.5.6. The requirements for the equipment needed to implement the solution (end-point/ peripherals/ software).

3.4.5.7. Is there a possibility of working on the basis of remote computing technology - Citrix XenApp/ XenDesktop version 7.15 and higher? Is

work in a remote computing environment possible in a Terminal Server configuration? Can the peripheral devices work compatibly with a Citrix XenApp configuration?

3.4.5.8. Can interfacing to the organization's systems be implemented via an API?

3.4.5.9. How is the application designed so that it works well in a shared resources environment, without interfering with the other applications running on the same server?

3.4.5.10. Which operating systems are used?

3.4.5.11. Which databases does the system use?

3.4.5.12. Is the proposed product supported in future standard Microsoft Windows environments? In the response, describe additional environments that the product is compatible with, if any.

3.4.5.13. The Israel Police has an organizational standard for the procurement of servers. The Company shall specify whether the application can be installed on police infrastructures. What resources are required for this purpose? If not, specify what is required in hardware and applicative terms to implement the application.

3.4.5.14. Servers - the server array at the Israel Police supports high-availability and a VMware-based virtual infrastructure. In parallel to the Israel Police, how is the server array built in this application?

3.4.5.15. What is the minimum physical working configuration in terms of processing power, memory, etc. (for the servers)?

3.4.5.16. Method of operation. Will it exist in a stretch site configuration by normal running of the application on two sites simultaneously and splitting the loads (in an active/active configuration) or in a different configuration? Can the 2 sites be logged in to concurrently in a configuration of Layer2 over layer3

3.4.5.17. Can work be done on both sites concurrently? What are the syncing capabilities between the two sites?

3.4.5.18. Is load-balancing executed? F5 Gslb?

3.4.5.19. How does the system support survivability and continuity of service solutions in the event of a fault? Does survivability and redundancy exist for all the components of the infrastructure, including the storage machines and the communications switches? (Details required).

3.4.5.20. How is the data storage process done, and by which company? Will central storage be enabled on storage machines based on Hitachi SAN technology connected to storage switches operating on Brocade SAN technology?

3.4.5.21. What are the workstations and what is their processing power?

3.4.5.22. The accompanying command-and-control system - how is the process of monitoring the infrastructure components implemented? Can Microsoft SCOM 2012 and Zabbix products be used?

Can SCOM 2012 command-and-control agents be installed (including future versions)?

3.4.5.23. Can Key Performance Indicators (KPI) be defined.

3.4.5.24. Are applicative components monitored, and does the system support sending of alerts to the command-and-control system by means of SNMP or by running additional alerting tools (dll, exe or Web Service).

3.4.5.25. Provide details about the backup system and the backup software that are used. Will support backed up by virtual infrastructure Snap be possible?

3.4.5.26. The Israel Police computing environment is a closed environment that does not enable access to the Internet or to any other external communications network. Is an Internet connection required to run the software?

3.4.5.27. How is backup of the system performed? Which software is used?

3.4.6. **Support and maintenance services**

3.4.6.1. Details about the system's expected lifecycle, including how long it can function without the need for a significant upgrade, as well plans for future upgrades.

3.4.6.2. The type of technical support that the system requires.

3.4.6.3. The manufacturer's policy for distributing versions, builds and updates.

4. Instructions for preparing the response to the RFI

4.1. The response can refer to more than one service/ product/ model. A participant who submits a response that addresses more than one service/ product/ model shall complete Annexes A, B and C for each proposed service/ product/ model separately.

4.2. The participant shall present any additional information that it deems relevant to this RFI.

4.3. The Israel Police may request any additional information in order to examine the response.

4.4. Should supplementary documents be required, the Israel Police may enable a participant to produce them within a timeframe as shall be determined.

4.5. The participant shall transfer general data (company registration number/ authorized dealer number, number of employees, whether the participant is a manufacturer and/or sole agent and/or representative in Israel for the manufacturer, etc).

4.6. The response to section 3.3.1 shall be submitted in the form of a table as specified in Annex A.

4.7. The response to section 3.3.2 shall be submitted in the form of a table as specified in Annex B.

4.8. The response to section 3.4 shall be submitted in the form of a table as specified in Annex C. In the response, the participant shall indicate in the table compliance of the proposed product/ service that it shall present with the required capabilities.

The response table shall include the following column headings:

4.8.1. The section number, as presented in this document.

4.8.2. The essence of the requirement that appears in this document.

4.8.3. The product/ service's compliance with the requirement: meets/ does not meet.

4.8.4. Details about the product/ service's meeting of the requirements specified in this document.

4.8.5. Referral to the details of the capability in the documents of the response.

5. Presentation and demonstration (RFD)

5.1. The presentation and demonstration stages are optional. The Israel Police reserves the right to have a presentation and demonstration, at its professional and budgetary discretion, taking into consideration the requirements in this document, and subject to the responses.

5.2. It is hereby clarified that the intention of the presentation and demonstration is to learn about the existing capabilities and possibilities in the market, and will only constitute a preliminary stage in a decision on whether and how to conduct the procurement on a specific issue, and in order to draw up the terms and conditions of a future contractual engagement.

5.3. If a demonstration is conducted, it will be for those responses that comply with the system's requirements according to the needs of the Israel Police, subject to a decision and approval of the Tenders Committee.

5.4. Should the Israel Police decide to have a demonstration, the demonstration will be conducted in Israel or elsewhere in the world where the system is installed, at a time that shall be coordinated between the Israel Police and the respondent.

5.5. For the avoidance of doubt, a presentation or demonstration does not constitute a contractual engagement to execute a transaction; it is simply intended for the purposes of illustration and to learn about the market. Accordingly, these proceedings cannot be extended or contractually expanded. according to Regulation 3(4) of the Mandatory Tenders Regulations.

5.6. It is hereby clarified that the Israel Police will not make any payment on its part, and the participant will bear all the costs and expenses arising from the presentation and/or demonstration, if any, apart from accommodation and travel expenses from abroad.

5.7. **The presentation stage:**

5.7.1. Following examination of the response documents and receipt of the Tenders Committee's approval, all the relevant responses can be transferred to the presentation stage.

5.7.2. Any participant that met the aforesaid requirements will present the system that is the subject of the response to the Israel Police, including a detailed professional explanation about the proposed system's capabilities.

5.7.3. Should the Israel Police decide to hold a presentation, the presentation will be conducted in Israel. In cases where the system cannot be brought to Israel for presentation, the option will be provided of making a remote presentation of the system (on Zoom, in a video conference, or in another way).

5.7.4. The system presentation will be made within a timeframe does not exceed 4 weeks from the Israel Police's announcement. The Israel Police may extend the timeframe by another two weeks, at its sole discretion, subject to the approval of the Israel Police Tenders Committee.

5.8. The demonstration stage:

5.8.1. Requirements for advancing to the demonstration stage:

5.8.1.1. The 3 responses with the highest scores, according to the point scoring specified below and in Annex D will advance to the demonstration stage.

5.8.1.2. The following are the mandatory requirements and the parameters for the scoring of the response in order to advance to the demonstration stage:

5.8.1.2.1. The participant is the manufacturer of the system that is the subject of this response, or the manufacturer's authorized representative (mandatory requirement - 15 points).

5.8.1.2.2. The system is standard certified for criminal AFIS fingerprint systems (mandatory requirement - 10 points).

5.8.1.2.3. The system has been examined in the past 3 years at least in an accuracy audit conducted by one or more international standards organizations (such as FBI, NIST/ ANSI) (mandatory requirement - 10 points).

5.8.1.2.4. The system has the certification of an information security and cybersecurity standard, such as: NIST, ISO, SOC2, GDPR (mandatory requirement - 10 points).

5.8.1.2.5. The system manufacturer has at least 5 years' experience (2020-2024 inclusive) in the manufacture, installation, operation and maintenance of criminal AFIS systems (mandatory requirement - 15 points).

5.8.1.2.6. The manufacturer has different customers at which a criminal AFIS system has been installed, and it has been providing them with full maintenance services for at least the 5 past years (one point per customer, maximum of 10 points).

5.8.1.2.7. The manufacturer supplied and installed 3 criminal AFIS systems in European Union member states and/or in the United

States and/or in Canada and/or in Australia and/or in New Zealand (5 points per system, maximum of 15 points).

5.8.1.2.8. The manufacturer has at least 3 customers at which a criminal AFIS has been installed that includes a repository of at least 4,000,000 fingerprint records (5 points per customer, maximum of 15 points).

5.8.1.2.9. Regarding section 5.8.1.2.5. The experience requirement will be deemed to have been met also in the case where the manufacturer underwent restructuring in the past (for example: acquisition of an operation, incorporation as a company, restructuring or consolidation of companies in another manner), such that the relevant operations were integrated in the manufacturer.

5.8.2. Following examination of the responses against the aforementioned requirements and receipt of the Tenders Committee's approval, the 3 responses with the highest scores, and that also met the mandatory requirements specified in section 5.8.1 and in all its subsections, will advance to the demonstration stage, as detailed below

5.8.3. The duration of the demonstration will be 2 workdays, subject to the discretion of the Israel Police, as necessary.

5.8.4. The system usage shall include the following capabilities at the very least:

5.8.4.1. TP-TP function.

5.8.4.2. TP-UL function.

5.8.4.3. LT-TP function.

5.8.4.4. PL-TP function.

5.8.4.5. LT-UL function.

5.8.4.6. PP-ULP function.

5.8.4.7. LP-ULP function.

5.8.4.8. Coding from within an image function.

5.8.4.9. The ability to define a closed group and to perform a search against that group only (Close search), using the function: LT-TP, LP-PP, LP-ULP, TP-TP, LT-UL, TP-UL.

5.8.5. During the demonstration, system usage will include full demonstration of the capabilities of all the stationary and mobile end-point stations that the system has, in the following stations at least:

5.8.5.1. Admin Station.

5.8.5.2. Full Expert Station.

5.8.5.3. Remot Scan station.

5.8.5.4. Fast ID Mobile Devies.

5.8.5.5. Mobile Device - a portable terminal for scanning and identifying latent prints at the scene of a crime in real time.

5.8.5.6. Life Scan Station.

5.8.6. During the demonstration period, the participant shall provide technical support and professional training, as necessary.

5.8.7. It is hereby clarified that the Israel Police will not make any payment on its part, and the participant will bear all the costs and expenses incurred in the demonstration, if any, apart from expenses for traveling abroad and accommodation.

5.8.8. **Insurance**

5.8.8.1. The participant in the demonstration will be required to sign an insurance annex, as specified in Annex E attached.

5.8.8.2. The participant shall sign this Annex as proof that it has read it in order to prepare and undertake to meet the insurance requirements should it participate in the demonstration stage.

5.8.8.3. The participant shall purchase and uphold all the insurance arrangements specified in "The Tender Insurance Requirements" Annex throughout the entire period of the demonstration with the State of Israel - the Israel Police and the Ministry of National Security, including all its agencies (as applicable), and as long as its responsibility exists.

5.8.8.4. The participant shall transfer to the Israel Police a certificate confirming the existence of the insurance policies in the standard text, signed by the insurer, as specified in the Insurance Requirements Annex in Annex E.

6. The information transfer process, and the timetable for execution

6.1. The participants are required to transfer their response by 12:00 noon on the date 13.8.25.

6.2. The detailed response to the aforementioned requirements can be transferred via the governmental "Challenging Arena" (Zira Haetgarit) website at https://hazira.gpa.gov.il/subdomain/afis-automated-fingerprint/end/campaign_overview?qmzn=MpTBqV , or alternatively, by electronic mail to: revitalc@police.gov.il

6.3. If necessary, the Israel Police may contact the participants for clarification and for supplementary information and for any other additional technical material.

6.4. If you have any questions or seek clarification, contact the governmental "Challenging Arena" (Zira Haetgarit) at the above website address by 12:00 noon on the date 3.7.25 or at the above electronic mail address.

6.5. The RFI is published in Hebrew and English. The wording and interpretation of the Hebrew prevail.

Annex A

Response to RFI Table - The System Manufacturer's Experience

In the response table, the participant shall provide a brief summary of the information required and shall elaborate as much as possible

A brief summary of the information required	Detailed response	Remarks
The name of the system manufacturing company, company registration number and place of residence		
Contact person's details and ways of communicating with the company's representative		
Company description and field of operations		
The company's experience (the number of years that the system manufacturer has engaged in the field of criminal AFIS systems)		

Details of the systems that are manufactured by the company		
The scope of its customer base		

Participant's name (first and last name)	**Phone**	**The participant's signature and stamp**

Annex B

Response to RFI table

List of customers - list of law enforcement bodies and units worldwide that use the system

In the response table, the participant shall provide a brief summary of the information required and shall elaborate as much as possible

	System No. 1	System No. 2	System No. 3	Remarks
Customer's name and country (in the event of mandatory confidentiality, provide details about the type of customer and general information)				
Customer contact person's details and ways of communicating				
The system version				
The database type				
The type of controlled information				
The size of the database				
Fingerprint system standards that the system is compliant with				
Information security standards that the system is compliant with				
Results of accuracy audits conducted in the past 3 years				
The size of the repository				
The amount of time it takes to set up the system until it becomes operational				
How long the system has been in use at the customer				
The manner in which the maintenance services are provided				

Participant's name (first and last name)	Phone	The participant's signature and stamp

Annex C

Information about the system's capabilities, and the support and maintenance infrastructures

The section number, as presented in this document.	The essence of the requirement that appears in this document.	The product/ service's compliance with the requirement: Meets/ Does not meet	Details about the product/ service's meeting of the requirements specified in this document	Referral to the detailed capability in the response documents
3.4.1	General description of the system, technical (hardware and software) and functional review.			
3.4.1.1	Possible sources of enrollment and input of ten prints (live scan stations, scanning of prints, external media, interfaces, crime scenes, etc.).			
3.4.1.2	Possible sources of enrollment and input of ten prints (live scan stations, scanning of prints, external media, interfaces, crime scenes, etc.).			
3.4.1.3	Authenticating/ identifying a person or latent prints, on the basis of fingerprints from different sources (interfaces, mobile/ cellular devices, etc.),			

	against a database, with emphasis on the following functions:			
*	TP-TP function.			
*	TP-UL function.			
*	LT-TP פונקציית function.			
*	PL-TP function.			
*	LT-UL function.			
*	PP-ULP function.			
*	LP-ULP function.			
*	Coding of TP from within image function.			
*	Ability to define a closed group and to perform a search against this group only (Close search), using the function: LT-TP, LP-PP, LP-ULP, TP-TP, LT-UL, TP-UL.			
3.4.1.4	Details of performance, response times, system's level of accuracy as a function of the search servers, their processing capacity and the quality and accuracy of the algorithm.			
3.4.1.5	Details about the ability of the system to integrate with external systems, including protocols supported, such as SDK and API. The company shall provide details about its experience in			

	implementing interfaces to the systems of international law enforcement agencies.			
3.4.1.6	Coding of finger and palm prints of a person from a photograph taken with a camera.			
3.4.1.7	Documenting and recording of fingerprints on the scene (prints and latent prints), using a mobile device, and sending them to the central system from different sources.			
3.4.1.8	Taking photographs of people's faces and storing the images as part of the Metadata; advanced image processing capabilities.			
3.4.1.9	Details of the functions for processing, matching, analyzing and updating fingerprints and latent prints, by an expert.			
3.4.1.10	Details of performance of the work process by a second expert on the screen, using ACE-V charting, and processing of the information, in order to present it in a court of law.			
3.4.1.11	Generation of queries and reports - details of all the possibilities available for generating various reports in the			

	system, including details of these capabilities using artificial intelligence (AI).			
3.4.1.12	System administration - details of the system admin station capabilities also address the ability to define profiles and different privileges for different users.			
3.4.1.13	Training and integration - details of the means of training and practicing on the system (stations, hardware and software), for the different stations and different operators.			
3.4.1.14	Test environment - the company shall present the solution proposed for setting up a system test environment.			
3.4.2	End-point stations			
3.4.2.1	The participant shall provide information about the hardware and software solutions for the end-point stations specified in section 2.4 above, and for additional end-point stations, if any, with respect to the system that is the subject of the response, with emphasis on the following topics:			
*	Technical specification for the computer. Is the application supported by standard computer stations.			
*	Operating system supported. Is the station			

	supported by a Microsoft environment, and by the various versions of Microsoft's operating systems.			
*	Types of fingerprint scanners including standards supported, with emphasis on an FBI standard.			
*	Biometric camera (resolution and standards supported).			
*	AI capabilities.			
*	Support for off-line mode.			
*	Biometric data encryption capabilities in the station.			
*	Control of user logins and privileges.			
*	How software updates are distributed.			
3.4.2.2	Mobile devices - fingerprint scanners and portable terminals			
*	Fast ID device designed to authenticate or identify a person.			
*	Details about the live scan surface, with emphasis on the physical size of the device, the size of the surface and the resolution.			
*	The participant shall describe the device's technical data and whether it includes a standard API for			

	developing interfaces and an SDK for development work.			
*	The manner of the connection (standard USB, type c) for the end-point unit, such as a computer, tablet.			
*	The operating system supported by the device (Windows, android, etc.)			
*	Does the device support CITRIX (Citrix) Terminal Server			
3.4.2.3	Portable terminal/ tablet for Fast ID			
*	The participant shall describe the device, with emphasis on the following functions:			
*	Checking against a local repository (Wanted List), as well as against a central database via the Israel Police's internal communications and via cellular communication.			
*	Does the portable terminal include a contact/ contactless smart card reader.			
*	The operating system supported by the portable terminal.			
*	The types of the connections on the portable terminal.			
*	The level of impermeability to moisture and dust			

*	Ability to withstand high temperatures.			
*	Details of the battery's capabilities			
3.4.2.4	Mobile station to enroll fingerprints from bodies			
*	Details of the mobile system, which will be able to take fingerprints directly from bodies and identify the prints against a mobile repository and against the central database.			
*	Including all the components needed to perform all the actions required to enroll fingerprints from bodies.			
3.4.2.5	A mobile device to photograph fingerprints at the scene of a crime			
3.4.3	Data migration			
3.4.3.1	Description of the data migration capabilities and of the migration process from an existing system to the system that is the subject of this response, with emphasis on the following repositories:			
3.4.3.1.1	Repository of fingerprints and palm prints from different sources, that were processed during their entry into and saving in the system.			
2.3.4.3.1	Database of latent finger and palm prints that underwent processing during their entry into and saving in the system.			

3.4.3.2	Database cleansing capabilities during the migration.			
3.4.3.3	Ability to use AI in the data migration process.			
3.4.3.4	The preparations required of the supplier of the system being migrated for purposes of the migration.			
3.4.3.5	The company shall specify its experience in migrating the data of a system containing at least 3,000,000 ten prints and 250,000 latent fingerprints, with emphasis on the following parameters:			
1.3.4.3.5	Details of the customers and the customers' contact persons (in the event of mandatory confidentiality, provide details on the type of customer and general information).			
.3.4.3.5	The manufacturer of the system from which the data were migrated.			
3.4.3.5	Type of database			
.3.4.3.5	How long it took to perform the migration.			
.3.4.3.5	The manner of the transition from the old system to the new one, including reference to functional continuity.			
3.4.4	Information security and cybersecurity			
3.4.4.1	Details of information security and cybersecurity standards that the organization			

	and the system are compliant with, such as NIST, ISO, SOC2, GDPR, etc.			
3.4.4.2	Information security and cybersecurity controls in use in the system/ service.			
3.4.4.3	Manner of integration of the SDLC process in the lifecycle of the system/ service, including software testing.			
3.4.4.4	If the participant proposes using the IT infrastructure of another supplier, it must state this and attach a document describing how the responsibility is split between it and the additional infrastructure supplier, and what measures it takes to protect the data from vulnerability at the infrastructure level.			
3.4.4.5	Details of the implementation and manner of support for the monitoring and control systems, for the transfer of log and events files to automation and security monitoring systems, such as SIEM and SOAR, e.g. SYSLOG.			

3.4.4.6	Details of the system's support for authentication mechanisms such as SSO and IAM.			
3.4.4.7	Details as to whether the system includes the possibility of a biometric check for authorization to log in to the system.			
3.4.4.8	Details about the system's support for imposing a password changing policy that includes defining of variables such as: length, complexity, expiry, history, MFA enforcement, etc.			
3.4.4.9	Details of how the system supports Least Privilege access for users for the actions they are allowed to perform in the system, in order to protect the data against unauthorized access, exposure, tampering, modification or deletion.			
3.4.4.10	Details of all the encryption protocols that exist in the system (including type of encryption, such as AES 256 bit, and key size, such as 2048 bits or greater), for end-to-end data encryption, and data encryption both in transit and at rest.			

3.4.4.11	Details of the system's support for storing encryption keys in hardware security modules (HSM) and key management services (KMS) and/or any other solution that secures keys. The Company shall specify how this response is implemented. The Company shall specify any additional information about information security and cybersecurity relating to the system.			
3.4.5	The system infrastructures			
3.5.5.1	Information about the hardware requirements, the operating system and network infrastructures required.			
3.5.5.2	The communications solution for working in an ACTIVE-ACTIVE configuration, including definition of traffic files required between the sites.			
3.5.5.3	The volume and data transfer rate of the files and the minimum bandwidth that enables normal operation. Note that the company will be required to work on the basis of the active infrastructure that			

	exists at the Israel Police.			
3.5.5.4	The company shall specify the manner of the response - web solution/ installation of local software (client) / CITRIX.			
3.5.5.5	Situation in which communication between the core and the end-point station is disconnected.			
3.5.5.6	The requirements for the equipment needed to implement the solution (end-point/ peripherals/ software).			
3.5.5.7	Is there a possibility of working on the basis of remote computing technology - Citrix XenApp/ XenDesktop version 7.15 and higher? Is work in a remote computing environment possible in a Terminal Server configuration? Can the peripheral devices work compatibly with a Citrix XenApp configuration.			
3.5.5.8	Can interfacing to the organization's systems be implemented via an API?			
3.5.5.9	How is the application designed so that it works well in a shared resources environment,			

	without interfering with the other applications running on the same server.			
3.5.5.10	Which operating systems are used			
3.5.5.11	Which databases does the system use?			
3.5.5.12	Will the proposed product be able to work/ be supported in future standard Microsoft Windows environments. In the response, describe additional environments that the product is compatible with, if any.			
3.5.5.13	The Israel Police has an organizational standard for the procurement of servers. The Company shall specify whether the application can be installed on police infrastructures. What resources are required for this purpose? If not, specify what is required in hardware and applicative terms to implement the application.			
3.5.5.14	Servers - the server array at the Israel Police supports high-availability and a vmware-based virtual infrastructure. In parallel to the Israel Police, how is the server array built in this application?			

3.5.5.15	What is the minimum physical working configuration in terms of processing power, memory, etc. (for the servers).			
3.5.5.16	Method of operation. Will it exist in a stretch site configuration by normal running of the application on two sites simultaneously and splitting the loads (in an active/active configuration) or in a different configuration? Can the 2 sites be logged in to concurrently in a configuration of Layer2 over layer3			
3.5.5.17	Can work be done on both sites concurrently? What are the syncing capabilities between the two sites?			
3.5.5.18	Is load-balancing executed? F5 Gslb?			
3.5.5.19	How does the system support survivability and continuity of service solutions in the event of a fault. Does survivability and redundancy exist for all the components of the infrastructure, including the storage machines and the communications			

	switches? (Details required).			
3.5.5.20	How is the data storage process done, and by which company. Will central storage be enabled on storage machines based on Hitachi SAN technology connected to storage switches operating on Brocade SAN technology?			
3.5.5.21	What are the workstations and what is their processing power?			
3.5.5.22	The accompanying command-and-control system - how is the process of monitoring the infrastructure components implemented? Can Microsoft SCOM 2012 and Zabbix products be used?			
3.5.5.23	Can Key Performance Indicators (KPI) be defined.			
3.5.5.24	Are applicative components monitored, and does the system support sending of alerts to the command-and-control system by means of SNMP or by running additional alerting tools (dll, exe or Web Service).			
3.5.5.25	Provide details about the backup system and the backup software that are used. Will support backed up by			

	virtual infrastructure Snap be possible?			
3.5.5.26	The Israel Police computing environment is a closed environment that does not enable access to the Internet or to any other external communications network. Is an Internet connection required to run the software?			
3.5.5.27	How is backup of the system performed? Which software is used			
3.4.6	Support and maintenance services			
3.4.6.1	Details about the system's expected lifecycle, including how long it can function without the need for a significant upgrade, as well plans for future upgrades.			
3.4.6.2	The type of technical support that the system requires.			
3.4.6.3	The manufacturer's policy for distributing versions, builds and updates.			

Annex D

Scoring Table - advancing to the demonstration stage

Section in the RFI	Summary/ heading	Maximum points	Score	Required
5.8.1.2.1	The participant is the manufacturer of the system that is the subject of this response, or the manufacturer's authorized representative (mandatory requirement).	15		Furnishing of a certificate
5.8.1.2.2	The system is standard certified for criminal AFIS fingerprint systems (mandatory requirement).	10		Furnishing of a certificate
5.8.1.2.3	The manufacturer's criminal AFIS system has been examined in the past 3 years at least in an accuracy audit conducted by one or more international standards organizations (such as the FBI, NIST/ ANSI) (mandatory requirement).	10		Furnishing of a certificate
5.8.1.2.4	The system has the certification of an information security and cybersecurity standard, such as: NIST, ISO, SOC2, GDPR (mandatory requirement).	10		Furnishing of a certificate
5.8.1.2.5	The system manufacturer has at least 5 years' experience (2020-2024 inclusive) in the manufacture, installation, operation and maintenance of criminal AFIS systems (mandatory requirement).	15		Furnishing of a certificate
5.8.1.2.6	The manufacturer has different customers at which a criminal AFIS system has been installed, and it has been providing them with full maintenance services for at least the 5	10		Furnishing of a certificate

Section in the RFI	Summary/ heading	Maximum points	Score	Required
	past years (one point per customer, maximum of 10 points)			
5.8.1.2.7	The manufacturer has supplied and installed 3 criminal AFIS systems in European Union member states and/or in the United States and/or in Canada and/or in Australia and/or in New Zealand (5 points per system, maximum of 15 points)	15		Furnishing of a certificate
5.8.1.2.8	The manufacturer has at least 3 customers at which a criminal AFIS has been installed that includes a repository of at least 4,000,000 fingerprint records (5 points per customer, maximum of 15 points)	15		Furnishing of a certificate

Attn Annex E

The State of Israel - Israel Police
National Headquarters, Ramla, 41 Ba'alei HaMelacha St.

Dear Sir/ Madam

Contractual Engagement General Insurance Annex

The participant undertakes to draft and maintain insurance policies commensurate with the services and/or works that are the subject of this agreement for the State of Israel – the Israel Police (hereinafter "the Customer"), as is customary in their field of activity (for example: employer's liability insurance, third-party liability insurance, heavy equipment insurance, property insurance, goods in transit insurance, or any other insurance, as applicable) within reasonable limits of liability according to the nature and scope of the services and/or the works that are the subject of this agreement. Should the participant engage subcontractors, it must ensure that its insurance policies include cover of its liability in respect of them, and it must require them to draft insurance policies to cover their direct liability, as required in this Annex. Alternatively, the participant shall make sure that its insurance policies include cover of its operations and its direct liability.

The participant shall ensure that in all the insurance policies that it has drafted in accordance with this Annex (apart from contractor's/ construction insurance), the Customer is added as another insured under the extension of indemnity as is customary for that type of insurance.

The participant shall ensure that contractors'/ construction insurance, to the extent that it has been drafted in respect of the services and/or the works that are the subject of this agreement, the Customer is included as well as all the contractors and subcontractors, as additional insured.

The participant shall ensure that all the insurance policies that are drafted under this Annex, include a clause waiving the right to subrogation/ revocation towards the Customer and its employees (this waiver will not apply towards a person who caused damage maliciously) and a clause according to which the insurance policies will come before and be primary without the right of contribution and/or recourse.

For the avoidance of doubt, the participant is solely liable towards the insured for paying the insurance premiums, the deductibles for all the policies and for fulfilling all the obligations imposed on the insured according to the insurance policies' conditions.

The Israel Police reserves the right to obtain from the participant a certificate confirming the existence of the insurance or copies of the policies, from time to time and on demand.

Noncompliance with the terms of this Annex constitutes a violation of this agreement.

Date	**Name of participant (first and last name)**	**The participant's signature and stamp**