משטרת ישראל

מטא"ר / אגף תמיכה לוגיסטית
מחלקת רכישות ומכירות
מדור רכש טכנולוגי
טלפון: 08-9124130
27.3.2025

הנדון: <u>פניה מוקדמת לקבלת מידע (RFI/ RFD) - מספר 6/2025</u>

<u>הליך לבקשת מידע, הדגמה והצגת יכולות בנושא:</u>

<u>מערכת אפיס - AFIS (Automated Fingerprint Identification System)</u>

1. <u>כללי</u>

1.1. משטרת ישראל/חטיבת הזיהוי הפלילי, מעוניינת לקבל מידע על מערכת אפיס פלילית (מערכות המיועדות למשטרות וגורמי אכיפת חוק), אוטומטית, לזיהוי, השוואה ואגירה של טביעות אצבע וכפות ידיים - AFIS (Automated fingerprint identification system) (להלן: "מערכת אפיס") וכן לבצע הדגמה ככל שיידרש.

1.2. משטרת ישראל מעוניינת להישאר בחזית המערכות המתקדמות בעולם, בתחום ניהול טביעות אצבע פלילי ולהפעיל יכולות חדשניות ואיכותיות לפי צרכיה. לכן, מבוקש על ידי המשטרה, לבחון את הטכנולוגיות החדשות הקיימות בעולם בתחום מערכות האפיס (חומרה ותוכנה) ואת התאמתן לצרכי המשטרה. יובהר כי בקשת מידע זו מתייחסת למערכות אפיס בעלות יכולות ביחס לטביעות אצבע וכפות ידיים. בכל מקום בבקשה זו בו רשום "טביעות אצבע", הכוונה גם ליכולות ביחס לכפות ידיים.

1.3. על המשתתפים המעוניינים להשיב לפניה זו לפרט את מירב המידע שבידיהם הנוגע למוצר/שירות כאמור או תחליפו, ולמידת התאמת המוצר/השירות לצרכים המפורטים במסמך זה.

1.4. הליך ה-RFI אינו בבחינת הליך מכרזי ואין לראות בו משום הליך בחירת המוצר/השירות של המשתתף או בקשה לקבלת הצעות. כמו כן, אין לראות בפניה זו משום התחייבות כלשהי מצד משטרת ישראל כלפי המשתתפים בנוגע לפרסום מכרז או ביצוע פעילות המשך לתהליך זה, כולל RFD וביצוע רכש עתידי. אין בפניה זו כדי ליצור כל מחויבות חוזית בין משטרת ישראל לבין מי שהגיש מענה לפניה. לאחר קבלת המענים לפניה זו, משטרת ישראל תשקול את המשך פעולותיה בהתאם לשיקול דעתה הבלעדי.

1.5. במידה ומשטרת ישראל תחליט לקיים הליך של ביצוע הדגמות (RFD), הפניה תהיה למשתתפים אשר המענה מטעמם ל-RFI עונה על הצורך המוגדר בסעיף 5.8.1 ובהתאם להחלטת ועדת המכרזים ואישורה.

1.6. יובהר, כי כל התקשרות של משטרת ישראל כפופה לחוק חובת המכרזים, וכי אין בתהליך ה-RFI שיתקיים כדי לייתר תהליך של מכרז בהתאם לחוק חובת המכרזים, אם תחליט משטרת ישראל לקיימו. אין לראות בהשתתפות בהליך זה משום תנאי או התחייבות להשתתפות במכרז עתידי, אם

יתפרסם. כמו כן, אין בעצם המענה או בתוכן המענה לבקשה זו משום הקניית יתרון או חסרון כלשהו למי מהמשתתפים בתהליך זה.

1.7. במידה ומשטרת ישראל תחליט על רכישת מוצר/שירות כלשהו, הרכישה תתבצע בהתאם למפרט ספציפי שיכול להיות שונה מהדרישות במסמך זה.

1.8. כל ההוצאות הכרוכות במתן המענה לפניה זו, הן באחריות הבלעדית של המשתתפים ועל חשבונם, לרבות השלמות מידע, קיום פגישות ודיונים בנושא וכיו"ב. יודגש, כי המשתתפים לא יהיו זכאים לכל פיצוי או שיפוי בגין הוצאות ו/או נזקים שייגרמו להם בגין התייחסות לפניה, לרבות בקשר להצגה ו/או להדגמה ככל שתהיה.

1.9. בכפוף לאמור בסעיף 1.10 להלן, ולאחר בחינת המידע, משטרת ישראל תהא רשאית לעשות שימוש במידע שיתקבל מהמשתתפים כראות עיניה, לרבות לצורך בחינת האפשרות לבצע התקשרות בנושא ולגיבוש הדרישות בהתקשרויות כאמור, לצורך כתיבת מפרט ומכרז או כל מסמך אחר וכן לצורך הרכבת רשימת ספקים פוטנציאליים.

1.10. בכפוף לכל דין, משטרת ישראל תשמור את המידע שהגיע אליה במסגרת המענה בסודיות, וכן לא יעשה בו שימוש, כמפורט להלן:

1.10.1. לא תפרסם את המידע באופן פומבי.

1.10.2. לא תפגע בקניין הרוחני של נותן המענה.

1.10.3. לא תעשה בו שימוש מסחרי, למעט למטרות המנויות בבקשה.

1.10.4. לא תעביר את המידע לצד ג', למעט לגורם המעורב בהתקשרות, כגון, יועץ מקצועי.

1.11. על אף האמור בסעיף 1.10 לעיל, משטרת ישראל תהיה רשאית לפנות לנותן המענה בבקשה להשתמש במידע, באופן המוזכר בסעיפים 1.10.1-1.10.4.

1.12. בשל אילוצים שונים ייתכן שהליך זה יבוטל, או יצומצם או יידחה. משטרת ישראל לא תישא בכל הוצאה או תשלום בגין דחייה או ביטול או צמצום של ההליך או כל החלטה אחרת של משטרת ישראל בקשר להליך.

1.13. משטרת ישראל תהיה רשאית להאריך ו/או לדחות את המועדים הנקובים במסמך זה, בהתאם לשיקול דעתה הבלעדי.

1.14. משטרת ישראל שומרת לעצמה את הזכות לקיים פגישות הבהרה עם המשתתף, הכול בהתאם לשיקול דעתה.

1.15. משתתף המגיש מענה לפניה זו מצהיר כי:

1.15.1. הוא מסכים לכל המפורט במסמך ומתחייב שלא יהיו לו תביעות ו/או דרישות מאת משטרת ישראל או כל גורם אחר בקשר לשימוש במידע שיימסר על ידו.

1.15.2. אין במידע המוגש על ידי המשתתף או בשימוש עתידי בו כדי לפגוע בזכויות של צד שלישי, לרבות זכויות יוצרים, וכי הוא לבדו יישא באחריות לכל דרישה או תביעה שמקורה בטענה כי במסגרת שימוש במידע שהוגש הופרו זכויות צד שלישי כאמור, והוא ישפה את משטרת ישראל מיד עם קבלת הדרישה בגין כל סכום שיידרש ו/או יתבע לשלם מחמת תביעה או דרישה כאמור לעיל, לרבות הוצאות ושכ"ט עו"ד.

1.15.3. מסמכי פניה זו הינם רכושה הבלעדי של משטרת ישראל.

1.16. אין להתנות את המענה בתנאים כלשהם.

1.17. פניה זו תפורסם לאחר אישור של ועדת המכרזים של משטרת ישראל, ובפיקוחה.

2. <u>תיאור המערכת הקיימת</u>

2.1. ברשות משטרת ישראל מערכת אפיס פלילית גרסת CAFIS 6, אשר הותאמה לצרכי משטרת ישראל ומתוחזקת באמצעות חברת Thales. המערכת משמשת כמערכת פעילה מינואר 2014. הקמתה הושלמה והוכרזה מבצעית ב-1/2016.

2.2. **מטרת המערכת**:

טיפול מערכתי בכל הקשור לפעילות משטרת ישראל בתחום טביעות אצבעות וכפות ידיים לצורך העצמת היכולת לעיבוד והפקת ראיות, תפיסת חשודים והעמדתם לדין.

2.3. **ייעוד המערכת**:

2.3.1. ניהול טביעות האצבע במספר מאגרים.

2.3.2. הרכשה, עיבוד, אחסון, אחזור וניהול של טפסי טביעות אצבע של אדם, ממקורות שונים.

2.3.3. הרכשה, עיבוד, אחסון, אחזור וניהול של מעתקי טביעות אצבע ממעתקים, ממקורות שונים.

2.3.4. זיהוי חשודים וקשירתם לטביעות מזירות עבירה (מעתקים), תוך כדי היות החשוד בחזקת המשטרה בזמן אמת.

2.3.5. הרכשה, אחסון וניהול של תמונות ונתונים דמוגרפיים ופיזיים, כ-meta-data, בצמוד לטביעות האצבע.

2.3.6. זיהוי חללים וקורבנות אסון.

2.3.7. אימות/איתור וזיהוי אנשים ע"פ טביעות אצבע.

2.3.8. אימות/זיהוי אנשים נושאי ת"ז ביומטרית, ע"י השוואה ביומטרית מול נתוני תעודת הזהות.

2.3.9. התממשקות למערכות פנימיות של משטרת ישראל ולמערכות חיצוניות למשטרה כגון: מערכות FBI, INTERPOL, משרד הפנים וכד'.

2.4. **להלן פירוט עמדות הקצה הקיימות כיום במשטרת ישראל**:

2.4.1. עמדות מנהל מערכת - Admin Station.

2.4.2. עמדות מומחה אפיס - Work Station Expert.

2.4.3. עמדות הטבעה אלקטרו-אופטית - Live Scan.

2.4.4. עמדות לסריקת מעתקים וטפסי דיו - Remote Scan.

2.4.5. עמדות לזיהוי חללים - Victim Station.

2.4.6. עמדות מומחה מרוחקות - עמדות מומחה המאפשרות עבודה ניידת מכל מקום בעולם, הן ב-on-line מול המאגר המרכזי והן ב-offline מול מאגר מקומי - Portable Work Station Expert.

2.4.7. עמדות הטבעה מרוחקות - עמדות הטבעה המאפשרות עבודה ניידת מכל מקום בעולם, הן ב-on-line מול המאגר המרכזי והן ב-offline מול מאגר מקומי- Portable Live Scan.

2.4.8. סורקי ט״א בעמדות חוקר לאימות/אתור זהות (Fast Id), המופעלים ממערכות המשטרה. הסורקים כוללים קורא כרטיס חכם מובנה.

2.4.9. סורקי ט״א ניידים להתקנה בניידות משטרה, המופעלים ממערכות המשטרה, לצורך איתור/אימות זהות (Patrol car).

2.4.10. מסופון לזיהוי מהיר - Mobile Device.

2.4.11. מסופון לסריקה וזיהוי מעתקים בזירת עבירה בזמן אמת - Fusion Mobile Devise.

3. <u>תהליך קבלת המידע (RFI)</u>

3.1. המשתתפים יעבירו למשטרת ישראל מידע על המוצר/ים/השירות/ים מטעמם. המידע יכלול את מירב הפרטים והמסמכים.

3.2. **למענה יצורפו המסמכים הבאים <u>לפחות</u> (ניתן להגיש מסמכים באנגלית):**

3.2.1. מפרט המערכת נשוא המענה וכל מסמך אחר בו מפורטות יכולות המערכת.

3.2.2. אישור עמידה בתקנים למערכות טביעות אצבע בתחום האפיס הפלילי, בהם עומדת המערכת נשוא המענה.

3.2.3. תוצאות מבדקי דיוק של המערכת נשוא המענה, שנערכו ע״י אחד או יותר מארגוני התקנים הבינלאומיים (דוגמת FBI, ANSI/NIST) במהלך 3 השנים האחרונות.

3.2.4. אישור עמידה בתקני אבטחת מידע והגנת הסייבר, כגון: NIST, ISO, SOC2, .GDPR.

3.3. **מידע אודות ניסיון יצרן המערכת נשוא המענה והמשתמשים בה:**

3.3.1. <u>ניסיון יצרן</u>: ניסיון היצרן בפיתוח ותחזוקת מערכות אפיס, תוך התייחסות לשנות ניסיון, פירוט מערכות והיקף לקוחות.
ימולא בטבלה המצ״ב כ**נספח א׳**.

3.3.2. <u>פירוט לקוחות</u> (בדגש על גופי ביטחון במדינות חברות האיחוד האירופאי, ארה״ב, קנדה, אוסטרליה וניו-זילנד) אצלם מותקנת ומתוחזקת מערכת אפיס פלילי, בה מנוהל מאגר של יותר מ- 4,000,000 רשומות טביעות אצבעות.
ימולא בטבלה המצ״ב כ**נספח ב׳**.

3.4. **מידע אודות יכולות המערכת** (ימולא ע"ג נספח ג'):

3.4.1. **תיאור כללי של המערכת, סקירה טכנית (חומרה ותוכנה) ופונקציונלית בדגש על היכולות הבאות:**

3.4.1.1. מקורות הרכשה והזנה אפשריים של טפסי טביעות אצבע (עמדות הטבעה, סריקת טפסים, מדיה חיצונית, ממשקים, זירות עבירה וכו').

3.4.1.2. מקורות הזנה אפשריים של מעתקי טביעות אצבע (סריקת מעתקים, מדיה חיצונית, ממשקים, זירות עבירה וכו').

3.4.1.3. איתור ואימות זהות של אדם או מעתקים, על פי טביעות אצבע ממקורות שונים (ממשקים, רכיבים ניידים/ סלולאריים וכו'), מול המאגר, בדגש על הפונקציות הבאות:

- פונקציית TP-TP.
- פונקציית TP-UL.
- פונקציית LT-TP.
- פונקציית PL-TP.
- פונקציית LT-UL.
- פונקציית PP-ULP.
- פונקציית LP-ULP.
- פונקציית קידוד מתוך תמונה.
- אפשרות להגדרת קבוצה סגורה וביצוע החיפוש רק מול קבוצה זו (Close search), בפונקציית: LT-UL , TP-TP , LP-ULP , LP-PP , LT-TP , TP-UL.

3.4.1.4. פירוט ביצועים, זמני תגובה, רמת הדיוק של המערכת כפונקציה של שרתי החיפוש, יכולת העיבוד שלהם ואיכות דיוק האלגוריתם.

3.4.1.5. פירוט יכולת האינטגרציה של המערכת עם מערכות חיצוניות, כולל פרוטוקולים נתמכים כמו API ,SDK. החברה תפרט את ניסיונה במימוש ממשקים עם מערכות של גורמי אכיפת חוק בין - לאומיים.

3.4.1.6. קידוד טביעת אצבע וכף יד מאדם מצילום תמונה שצולם במצלמה.

3.4.1.7. תיעוד ורישום טביעות אצבע בשטח (טפסים ומעתקים), באמצעות רכיב נייד, ושליחתן למערכת המרכזית ממקורות שונים.

3.4.1.8. צילום פני אנשים ושמירת התמונה כחלק מ-Metadata, יכולות עיבוד תמונה מתקדמות.

3.4.1.9. פירוט הפונקציות לביצוע עיבוד, התאמה, פעולות ניתוח ועדכונים של טביעות אצבע ומעתקים, ע"י מומחה.

3.4.1.10. פירוט ביצוע תהליך עבודה של מומחה שני על המסך, על פי תהליך ACE-V עיבוד המידע, לצורך הצגתו בבית המשפט (Charting).

3.4.1.11. **הפקת שאילתות ודו"חות** - פירוט כל האפשרויות להפקת דוחות שונים במערכת, לרבות פירוט יכולות באמצעות בינה מלאכותית (AI).

3.4.1.12. **ניהול המערכת** - פירוט היכולות הקיימות בעמדת מנהל המערכת, יש להתייחס גם ליכולת להגדרת פרופילים והרשאות שונות למשתמשים השונים.

3.4.1.13. **הדרכה והטמעה** - פירוט אמצעי ההדרכה והתרגול במערכת (עמדות, חומרה ותוכנה), לעמדות השונות ולמפעילים השונים.

3.4.1.14. **סביבת בדיקות** - החברה תציג את הפתרון המוצע להקמת סביבת בדיקות למערכת.

3.4.2. **עמדות קצה**

3.4.2.1. המשתתף יספק מידע לפתרונות חומרה ותוכנה עבור עמדות הקצה המפורטות בסעיף 2.4 לעיל ועל עמדות קצה נוספות ככל שישנן בקשר למערכת נשוא המענה, בדגש על הנושאים הבאים:

- מפרט טכני למחשב, האם האפליקציה נתמכת בעמדות מחשב סטנדרטיות.
- מערכת הפעלה נתמכת, האם העמדה נתמכת בסביבת מייקרוסופט, מערכות הפעלה של מייקרוסופט וגירסאותיה.
- סוגי סורקי ט"א כולל תקנים נתמכים, בדגש על תקן FBI.
- מצלמה ביומטרית (רזולוציה ותקנים נתמכים).
- יכולות AI.
- תמיכה במצב לא מקוון.
- יכולות הצפנה על נתונים ביומטריים בעמדה.
- בקרת כניסה והרשאות משתמשים.
- אופן הפצת עדכוני תוכנה.

3.4.2.2. **רכיבים ניידים - סורקי ט"א ומסופונים**

רכיב לזיהוי מהיר המיועד לאימות זהות או איתור זהות של אדם:

- פירוט על משטח הטבעה בדגש על גודלו הפיזי של הרכיב, גודל המשטח ורזולוציה.
- המשתתף יתאר את הנתונים הטכניים של הרכיב והאם כולל API סטנדרטי לצורך פיתוח ממשקים ו- SDK לצורך פיתוח.
- אופן החיבור (USB סטנדרטי, Type c) ליחידת הקצה כגון מחשב, טאבלט.

- מערכות ההפעלה בהן הרכיב נתמך android , Windows וכד׳).
- האם הרכיב נתמך ב- CITRIX (Citrix) Terminal Server.

3.4.2.3. **מסופון/טאבלט נייד לזיהוי מהיר (Fast Id)**

המשתתף יתאר את הרכיב בדגש על הפונקציות הבאות:

- בדיקה מול מאגר מקומי (Wanted List) וגם מול מאגר המרכזי באמצעות תקשורת פנים משטרתית ותקשורת סלולארית.
- האם המסופון כולל קורא כרטיס חכם (Smart Card) מסוג contact / contactless.
- מערכת ההפעלה בה תומך המסופון.
- סוגי החיבורים במסופון.
- רמת האטימות בפני רטיבות ואבק.
- עמידות לטמפרטורה גבוהה.
- פירוט יכולות הסוללה.

3.4.2.4. **עמדה ניידת להרכשת ט״א מגופות**

- פירוט על מערכת ניידת אשר תוכל לבצע נטילת ט״א ישירות מגופות וזיהוי הטביעות מול מאגר נייד ומול המאגר המרכזי.
- כולל כל הרכיבים הנדרשים לצורך ביצוע כל הפעולות הנדרשות להרכשת ט״א מגופות.

3.4.2.5. **רכיב נייד לצילום ט״א בזירת עבירה**

- פירוט יכולות לרכיב נייד שישמש את חוקרי זירת העבירה השונים לצילום ט״א מזירת עבירה והעברתה למערכת המרכזית באמצעות תקשורת סלולארית לצורך חיפוש במאגר.

3.4.3. **הסבת נתונים**

3.4.3.1. תיאור יכולות הסבת הנתונים ותהליך ביצוע ההסבה ממערכת קיימת למערכת נשוא המענה, בדגש על המאגרים הבאים:

3.4.3.1.1. מאגר ט״א וכפות ידיים ממקורות שונים, אשר עברו עיבוד במהלך קליטתן ושמירתן במערכת.

3.4.3.1.2. מאגר מעתקי ט״א וכפות ידיים, אשר עברו עיבוד במהלך קליטתם ושמירתם במערכת.

3.4.3.2. יכולות טיוב המאגרים במהלך ההסבה.

3.4.3.3. יכולות שימוש ב- AI בתהליך הסבת הנתונים.

3.4.3.4. ההכנה הנדרשת מספק המערכת המוסבת לצורך ההסבה.

3.4.3.5. על החברה לפרט את ניסיונה בהסבת נתונים של מערכת הכוללת לפחות 3,000,000 טפסי ט״א ו-250,000 מעתקי ט״א, בדגש על הפרמטרים הבאים:

3.4.3.5.1. פרטי הלקוחות ואנשי קשר בלקוח (במידה של חובת חסיון - נא לפרט את סוג הלקוח ומידע כללי).

3.4.3.5.2. יצרן המערכת ממנה הוסבו הנתונים.

3.4.3.5.3. סוג בסיס הנתונים.

3.4.3.5.4. משך הזמן בו התבצעה ההסבה.

3.4.3.5.5. אופן המעבר בין המערכת הישנה לחדשה, תוך התייחסות לרציפות תפקודית.

3.4.4. **אבטחת מידע והגנת סייבר**

תיאור מאפייני השירות והמערכת בהתייחס לנושאי אבטחת מידע והגנת סייבר, בדגש על הפרמטרים הבאים:

3.4.4.1. פירוט תקני אבטחת מידע והגנת הסייבר שהארגון והמערכת עומדים בהם, כגון NIST, ISO, SOC2, GDPR וכד׳.

3.4.4.2. בקרות אבטחת המידע והגנת הסייבר אשר בשימוש המערכת/השירות.

3.4.4.3. אופן שילוב תהליך SDLC במחזור חיי המערכת/השירות כולל בדיקות תוכנה.

3.4.4.4. במידה והמשתתף מציע שימוש בתשתית מחשוב של ספק אחר, עליו לציין זאת ולצרף מסמך המתאר כיצד מתבצעת חלוקת האחריות בינו לבין ספק התשתית הנוסף ובאילו אמצעים הוא נוקט בכדי להגן על המידע מפני פגיעות ברמת התשתית.

3.4.4.5. פירוט יישום ואופן התמיכה במערכות ניטור ובקרה, בהעברת קבצי לוג ואירועים למערכות אוטומציה וניטור אבטחתי כגון SIEM ו- SOAR כגון SYSLOG.

3.4.4.6. פירוט תמיכת המערכת במנגנוני הזדהות כדוגמת SSO, IAM.

3.4.4.7. פירוט האם המערכת מכילה אפשרות לבדיקה ביומטרית כהרשאה לכניסה למערכת.

3.4.4.8. פירוט לגבי תמיכת המערכת בהחלת מדיניות החלפת סיסמאות, אשר תכלול קביעה של משתנים כגון: אורך, מורכבות, תוקף, היסטוריה, אכיפת MFA וכדומה.

3.4.4.9. פירוט אופן תמיכת המערכת בהרשאות גישה מצומצמות ככל האפשר (Least Privilege) לביצוע פעולות מורשות למשתמשי המערכת, בכדי להגן על הנתונים מפני גישה לא מורשית, חשיפה, שיבוש, שינוי או מחיקה.

3.4.4.10. פירוט כלל פרוטוקולי ההצפנה הקיימים במערכת (לרבות סוג ההצפנה לדוגמה AES 256bit וגודל מפתח לדוגמה 2048 ומעלה), עבור הצפנת המידע והתקשורת מקצה לקצה, הצפנת המידע הן בתנועה ובמנוחה.

3.4.4.11. פירוט תמיכת המערכת בשמירת מפתחות ההצפנה במערכות אבטחת חומרה (HSM) ושירותי ניהול מפתח (KMS) ו/או בכל פתרון אחר המספק הגנה על המפתחות. על החברה לפרט כיצד מיושם מענה זה.

החברה תפרט כל מידע נוסף שנוגע לאבטחת מידע והגנת הסייבר הקשור למערכת.

3.4.5. **תשתיות המערכת**

3.4.5.1. מידע על דרישות החומרה, מערכת ההפעלה ותשתיות רשת נדרשות.

3.4.5.2. מענה התקשורתי לעבודה בתצורת ACTIVE-ACTIVE לרבות הגדרת קבצי תעבורה נדרשים בין האתרים.

3.4.5.3. נפח וקצב העברת המידע של הקבצים ואת רוחב הסרט המינימאלי המאפשר עבודה תקינה. יצוין כי החברה תידרש לעבוד על בסיס התשתית האקטיבית הקיימת במשטרת ישראל.

3.4.5.4. על החברה לפרט את אופן המענה - פתרון WEB / התקנת תוכנה מקומית (קליינט) / CITRIX.

3.4.5.5. מצב של ניתוק תקשורת בין הליבה לתחנות הקצה.

3.4.5.6. דרישות הציוד הנדרשות ליישום הפתרון (קצה/ היקפי/ תוכנה).

3.4.5.7. האם יש אפשרות לעבודה על בסיס טכנולוגית מחשוב מרוחק - citrix xenapp/xendesktop גרסאות 7.15 ומעלה? האם יש אפשרות לעבודה בסביבת מחשוב מרוחק בתצורת Terminal Server? האם ההתקנים הפריפריאליים יכולים לעבוד בתאימות לתצורת ה- Citrix XenApp?

3.4.5.8. האם תיתכן התממשקות למערכות הארגון באמצעות API.

3.4.5.9. כיצד מתוכנן היישום כך שיפעל היטב בסביבת משאבים משותפים, ללא גרימת הפרעה ליישומים האחרים הפועלים על אותו שרת.

3.4.5.10. מהן מערכות ההפעלה בהן נעשה שימוש.

3.4.5.11. מהם מסדי הנתונים שבשימוש המערכת.

3.4.5.12. האם המוצר המוצע נתמך בסביבות Microsoft Windows סטנדרטיות עתידיות. יש לתאר במענה סביבות נוספות אשר המוצר מתאים עבורן, אם קיימות.

3.4.5.13. משטרת ישראל מקיימת סטנדרט ארגוני בכל הקשור ברכש שרתים. החברה תפרט האם היישום יכול להיות מותקן על גבי תשתית משטרתית? מה הם המשאבים

הנדרשים לכך? במידה ולא - נדרש לפרט מה נדרש חומרתית ואפליקטיבית ע"מ ליישם את האפליקציה.

3.4.5.14. שרתים - מערך השרתים במשטרת ישראל תומך ב High Availability וב-בתשתית וירטואלית מבוססת vmware. בהקבלה למשטרת ישראל, כיצד נבנה מערך השרתים ביישום הזה?

3.4.5.15. מה היא תצורת העבודה הפיזית המינימלית מבחינת כוח עיבוד, זיכרון ועוד (עבור השרתים).

3.4.5.16. שיטת ההפעלה. האם תתקיים בתצורת stretch site ע"י הפעלת היישום בשגרה בשני האתרים בו זמנית תוך חלוקת עומסים (בתצורת Active\Active) או בתצורה אחרת? האם קיימת יכולת התחברות ל-2 האתרים במקביל בתצורת רשת של Layer2 over layer3?

3.4.5.17. האם תיתכן עבודה בשני אתרים במקביל. מהן יכולות הסנכרון בין שני האתרים?

3.4.5.18. האם קיים איזון עומסים? F5 Gslb?

3.4.5.19. כיצד המערכת תומכת בפתרונות שרידות והמשכיות של השירות גם במקרה תקלה. האם קיימת שרידות ויתירות בכל רכיבי התשתית כולל מכונות האחסון ומתגי התקשורת? (נדרש לפרט).

3.4.5.20. כיצד מתבצע תהליך אחסון נתונים וע"י איזה חברה. האם תתאפשר שמירה מרכזית במכונות אחסון מבוססות בטכנולוגיה SAN של חברת Hitachi המחוברות למתגי אחסון העובדים בטכנולוגיה SAN של Brocade?

3.4.5.21. מה הן תחנות העבודה ומה כוח העיבוד בהן.

3.4.5.22. מערך השו"ב הנלווה - כיצד מתבצע תהליך ניטור רכיבי תשתית? האם תתכן שימוש במוצרי Microsoft SCOM 2012 ו- Zabbix.
האם סוכני שו"ב מסוג scom2012 יוכלו להיות מותקנים (כולל גרסאות עתידיות)?

3.4.5.23. האם ניתן להגדיר Key Performance Indicators (KPI).

3.4.5.24. האם קיים ניטור רכיבים אפליקטיביים וכן האם המערכת תתמוך בשליחת התרעות למערכת שו"ב ע"י SNMP או ע"י הפעלת כלי התראה נוספים (exe, dll או Web Service) .

3.4.5.25. פירוט אודות מערך הגיבוי ותוכנת הגיבוי בהם נעשה שימוש. האם תתאפשר תמיכה בגיבוי Snap של תשתית וירטואלית?

3.4.5.26. סביבת המחשוב המשטרתית הינה סביבה סגורה שאינה מאפשרת קישור לאינטרנט או לרשת תקשורת חיצונית אחרת. האם נדרש חיבור לאינטרנט לצורך הפעלת התוכנה?

3.4.5.27. כיצד מתבצע הגיבוי של המערכת? מה התוכנה בה משתמשים?

3.4.6. **שירותי תמיכה ותחזוקה**

3.4.6.1. פרטים אודות מחזור חיים צפוי של המערכת, כולל משך הזמן שבו תתפקד ללא צורך בשדרוג משמעותי וכן תכניות לשדרוגים עתידיים.

3.4.6.2. סוג התמיכה הטכנית הנדרשת למערכת.

3.4.6.3. מדיניות היצרן בנוגע להפצת גרסאות, תת-גרסאות ועדכונים.

4. <u>הנחיות להכנת המענה ל-RFI</u>

4.1. ניתן להעביר מענה המתייחס ליותר משירות/מוצר/דגם אחד. משתתף המעביר מענה המתייחס ליותר משירות/מוצר/דגם אחד, ימלא את הנספחים א', ב' ו-ג' עבור כל שירות/מוצר/דגם מוצע באופן נפרד.

4.2. המשתתף יציג כל מידע נוסף, שימצא כרלוונטי לפניה זו.

4.3. משטרת ישראל רשאית לבקש כל מידע נוסף לצורך בחינת המענה.

4.4. ככל ותידרש השלמת מסמכים, משטרת ישראל תהא רשאית לאפשר למשתתף להשלים את המצאתם בפרק הזמן אשר ייקבע.

4.5. המשתתף יעביר נתונים כלליים (מספר ח.פ/מספר עוסק מורשה, מספר עובדים, האם המשתתף הנו היצרן ו/או סוכן בלעדי ו/או מורשה בישראל של היצרן וכיוצא בזה).

4.6. המענה לסעיף 3.3.1 יוגש בתצורה של טבלה כמפורט בנספח א'.

4.7. המענה לסעיף 3.3.2 יוגש בתצורה של טבלה כמפורט בנספח ב'.

4.8. את המענה לסעיף 3.4 יש להגיש בתצורה של טבלה כמפורט בנספח ג'. המשתתף יציין בטבלת המענה את עמידת המוצר/שירות המוצע בדבר היכולות הנדרשות הקיימות במוצר/שירות אותו תציג.
טבלת המענה תכיל עמודות במבנה הבא:

4.8.1. מספר הסעיף כפי שהוא מוצג במסמך זה.

4.8.2. עיקר הדרישה המופיעה במסמך זה.

4.8.3. התאמת המוצר/השירות לדרישה: עונה/לא עונה.

4.8.4. פירוט עמידת המוצר/השירות בדרישות המפורטות במסמך זה.

4.8.5. הפניה לפירוט היכולת במסמכי המענה.

5. <u>הצגה והדגמה (RFD)</u>

5.1. שלבי ההצגה וההדגמה הינם אופציונאליים. משטרת ישראל שומרת לעצמה את הזכות לבצע הצגה והדגמה בהתאם לשיקול דעתה המקצועי והתקציבי, בהתחשב בדרישות מסמך זה ובכפוף למענים.

5.2. יובהר כי, הצגה והדגמה נועדו לצורך למידה על היכולות והאפשרויות הקיימות בשוק, ותהוונה שלב מקדים בלבד בעניין ההחלטה אם וכיצד לבצע רכש בנושא מסוים וכן לצורך גיבוש תנאי התקשרות עתידית.

5.3. ככל שתבוצע הדגמה, היא תבוצע בהתייחס למענים שמתאימים לדרישות המערכת לפי צרכי משטרת ישראל, ובהתאם להחלטת ועדת המכרזים ואישורה.

5.4. החליטה משטרת ישראל לבצע הדגמה, תיערך ההדגמה בישראל או במקום אחר בעולם בו מותקנת המערכת ובזמן שיתואם בין משטרת ישראל לנותן המענה.

5.5. למען הסר ספק, ביצוע הצגה או הדגמה אינו מהווה התקשרות לביצוע עסקה, אלא נועד אך ורק לצורך המחשה והליך למידה של השוק. בהתאם לכך, לא ניתן לבצע הארכה או הרחבת התקשרות להליך כאמור, בהתאם לתקנה 3(4) לתקנות חובת המכרזים.

5.6. יובהר כי משטרת ישראל לא תשלם כל תשלום מצידה והמשתתף יישא בכל העלויות וההוצאות הנובעות מההצגה ו/או ההדגמה ככל שיהיו, למעט הוצאות לינה ונסיעות מחוץ לארץ.

5.7. **שלב ההצגה:**

5.7.1. לאחר בחינת מסמכי המענה וקבלת אישור ועדת מכרזים, ניתן יהיה להעביר את כלל המענים הרלוונטיים לשלב ההצגה.

5.7.2. כל משתתף, שעמד בדרישות שלעיל, יציג את המערכת נשוא המענה למשטרת ישראל, תוך מתן הסבר מקצועי מפורט על יכולות המערכת המוצעת.

5.7.3. החליטה משטרת ישראל לבצע הצגה, תיערך ההצגה בישראל. במקרים בהם לא ניתן להביא מערכת להצגה בארץ, תינתן האפשרות להציג את המערכת בהצגה מרחוק (בזום, שיחת וידאו או בדרך אחרת).

5.7.4. הצגת המערכת תתבצע תוך פרק זמן שלא יעלה על 4 שבועות מרגע הודעת המשטרה. המשטרה תהיה רשאית להאריך פרק זמן זה בשבועיים נוספים, בהתאם לשיקול דעתה הבלעדי ובאישור וועדת המכרזים של המשטרה.

5.8. **שלב ההדגמה:**

5.8.1. **דרישות למעבר לשלב ההדגמה:**

5.8.1.1. לשלב ההדגמה יעברו 3 המענים בעלי הניקוד הגבוה ביותר בהתאם לניקוד כמפורט להלן ובנספח ד'.

5.8.1.2. להלן פרוט דרישות החובה ופרמטרים לניקוד המענה למעבר לשלב ההדגמה:

5.8.1.2.1. המשתתף הוא יצרן המערכת נשוא המענה או נציגות מורשית של היצרן (דרישת חובה - 15 נקודות).

5.8.1.2.2. המערכת בעלת תקן למערכות טביעות אצבע בתחום האפיס הפלילי (דרישת חובה - 10 נקודות).

5.8.1.2.3. המערכת נבחנה במהלך 3 השנים האחרונות לפחות במבדק דיוק אחד שנערך ע"י אחד או יותר מארגוני התקנים הבינלאומיים (דוגמת FBI, ANSI/NIST) (דרישת חובה - 10 נקודות).

5.8.1.2.4. המערכת בעלת תקן אבטחת מידע והגנת הסייבר, כגון: NIST, ISO, SOC2, GDPR (דרישת חובה - 10 נקודות).

5.8.1.2.5. ליצרן המערכת ניסיון של 5 שנים לפחות (2020-2024 כולל), בייצור, התקנה, הפעלה ותחזוקה של מערכות AFIS פלילי (דרישת חובה - 15 נקודות).

5.8.1.2.6. ליצרן לקוחות שונים אצלם הותקנה מערכת אפיס פלילי ולהם הוא מספק שירותי אחזקה מלאה ב-5 השנים האחרונות לפחות (נקודה אחת לכל לקוח, מקסימום 10 נקודות).

5.8.1.2.7. היצרן סיפק והתקין 3 מערכות אפיס פלילי במדינות האיחוד האירופאי ו/או בארה"ב ו/או בקנדה ו/או באוסטרליה ו/או בניו-זילנד (5 נקודות לכל מערכת, מקסימום 15 נקודות).

5.8.1.2.8. ליצרן לפחות 3 לקוחות אצלם מותקנת מערכת אפיס פלילי הכוללת מאגר של לפחות 4,000,000 רשומות טביעות אצבעות (5 נקודות לכל לקוח, מקסימום 15 נקודות).

5.8.1.2.9. לעניין סעיף 5.8.1.2.5 תיחשב דרישת הניסיון כמתקיימת, גם במקרה בו בעברו של היצרן התרחש שינוי ארגוני (לדוגמא: רכישת פעילות, התאגדות כחברה, רה-ארגון או איחוד של חברות בדרך אחרת), באופן בו הפעילות הרלוונטית השתלבה אצל היצרן.

5.8.2. לאחר בחינת המענים בדרישות המפורטות לעיל ולאחר קבלת אישור וועדת המכרזים, ניתן יהיה להעביר את 3 המענים בעלי הניקוד הגבוה ביותר, אשר גם עמדו בדרישות החובה כמפורט בסעיף 5.8.1 על תתי סעיפיו, לשלב ההדגמה כמפורט להלן

5.8.3. משך זמן ההדגמה יעמוד על 2 ימי עבודה, בכפוף לשיקול דעת משטרת ישראל בהתאם לצורך.

5.8.4. השימוש במערכת יכלול לפחות את היכולות הבאות:

5.8.4.1. פונקציית TP-TP.

5.8.4.2. פונקציית TP-UL.

5.8.4.3. פונקציית LT-TP.

5.8.4.4. פונקציית PL-TP.

5.8.4.5. פונקציית LT-UL.

5.8.4.6. פונקציית PP-ULP.

5.8.4.7. פונקציית LP-ULP.

5.8.4.8. פונקציית קידוד מתוך תמונה.

5.8.4.9. אפשרות להגדרת קבוצה סגורה וביצוע החיפוש רק מול קבוצה זו (Close search), בפונקציית: LT-UL , TP-TP , LP-ULP , LP-PP , LT-TP , TP-UL.

5.8.5. השימוש במערכת יכלול הדגמת יכולות מלאה לכל עמדות הקצה הקבועות והניידות שקיימות למערכת בעת ההדגמה ולפחות בעמדות הבאות:

5.8.5.1. עמדת מנהל מערכת.

5.8.5.2. עמדת מומחה.

5.8.5.3. עמדת שליחת תיקים.

5.8.5.4. רכיב לאימות זיהוי

5.8.5.5. רכיב לשליחת ממצאים מהשטח.

5.8.5.6. עמדת הטבעה.

5.8.6. במהלך תקופת ההדגמה, על המשתתף לספק תמיכה טכנית והדרכה מקצועית ככל שנדרש.

5.8.7. יובהר כי, משטרת ישראל לא תשלם כל תשלום מצידה והמשתתף יישא בכל העלויות וההוצאות הכרוכות בהדגמה ככל שתהיה, למעט הוצאות עבור נסיעות לחוץ לארץ ולינה.

5.8.8. **<u>ביטוח</u>**

5.8.8.1. המשתתף בהדגמה יידרש לחתום על נספח ביטוחי כמפורט בנספח ה' המצ"ב.

5.8.8.2. על המשתתף לחתום על נספח זה כראיה לעיונו לשם היערכות והתחייבות לעמידה בדרישות הביטוח בתנאי שישתתף בשלב ההדגמה.

5.8.8.3. על המשתתף לרכוש ולקיים את כל הסדרי הביטוח המפורטים בנספח "דרישות הביטוח במכרז" לאורך כל תקופת ההדגמה עם מדינת ישראל - משטרת ישראל והמשרד לביטחון לאומי על כל גופיו (ככל שרלוונטיים), וכל עוד אחריותו קיימת.

5.8.8.4. על המשתתף להעביר למשטרת ישראל אישור קיום ביטוחים בנוסח האחיד, חתום ע"י המבטחת, כפי שפורטו בנספח דרישות הביטוח בנספח ה'.

6. <u>תהליך העברת המידע, ולוחות זמנים לביצוע</u>

6.1. המשתתפים מתבקשים להעביר את המענה עד לתאריך 20.08.2025 בשעה 12:00.

6.2. את המענה המפורט לדרישות דלעיל ניתן להעביר באמצעות זירת האתגרים הממשלתית בכתובת:

https://hazira.gpa.gov.il/subdomain/afis-automated-fingerprint/end/campaign_overview?qmzn=MpTBqV

6.3. במידת הצורך, משטרת ישראל רשאית לפנות למשתתפים לצורך הבהרות והשלמות וקבלת חומר טכני או אחר נוסף.

6.4. לשאלות והבהרות ניתן לפנות בכתב בזירת האתגרים הממשלתית בכתובת המצויינת לעיל עד ליום 3.8.2025 בשעה 12:00 .

6.5. הפנייה פורסמה בעברית ובאנגלית, הנוסח והפרשנות בעברית גובר.

משטרת ישראל

נספח א'

טבלת מענה לקבלת מידע (RFI) - ניסיון יצרן המערכת

המשתתף יציין בטבלת המענה את תמצית המידע הנדרש וירחיב ככל שניתן

תמצית המידע הנדרש	מענה מפורט	הערות
שם החברה יצרנית המערכת, מס' ח.פ. ומקום מושבה		
פרטי איש קשר ודרכי התקשרות עם נציג החברה		
תיאור החברה ותחום פעילותה		
ניסיון החברה (שנות עיסוק יצרן המערכת בתחום מערכות AFIS פלילי)		
פירוט מערכות שמיוצרות ע"י החברה		
היקף לקוחות		

שם המשתתף (פרטי + משפחה)	טלפון	חתימה וחותמת המשתתף

משטרת ישראל

נספח ב'

טבלת מענה לקבלת מידע (RFI)

רשימת לקוחות - רשימת גופי אכיפת חוק ויחידות בעולם המשתמשים במערכת

המשתתף יציין בטבלת המענה את תמצית המידע הנדרש וירחיב ככל שניתן

	מערכת מס' 1	מערכת מס' 2	מערכת מס' 3	הערות
שם הלקוח והמדינה (במקרה של חובת חיסיון, נא לפרט את סוג הלקוח ומידע כללי)				
פרטי איש קשר בלקוח ודרכי התקשרות				
גרסת המערכת				
סוג בסיס נתונים				
סוג המידע המנוהל				
היקף בסיס הנתונים				
תקני מערכות טביעות אצבע בהם עומדת המערכת				
תקני אבטחת מידע בהם עומדת המערכת				
תוצאות מבדקי דיוק במהלך 3 השנים האחרונות				
היקף המאגר				
משך זמן הקמת המערכת עד הפעלתה המבצעית				
משך השימוש במערכת אצל הלקוח				
אופן מתן שירותי התחזוקה				

שם המשתתף (פרטי + משפחה)	טלפון	חתימה וחותמת המשתתף

משטרת ישראל

נספח ג'

מידע אודות יכולות המערכת, תשתיות תמיכה ותחזוקה

מספר הסעיף כפי שהוא מוצג במסמך זה.	עיקר הדרישה המופיעה במסמך זה.	התאמת המוצר/ השירות לדרישה: עונה/ לא עונה	פירוט עמידת המוצר/ השירות בדרישות המפורטות במסמך זה	הפניה לפירוט היכולת במסמכי המענה
3.4.1	תיאור כללי של המערכת, סקירה טכנית (חומרה ותוכנה) ופונקציונלית .			
3.4.1.1	מקורות הרכשה והזנה אפשריים של טפסי טביעות אצבע (עמדות הטבעה, סריקת טפסים, מדיה חיצונית, ממשקים, זירות עבירה וכו').			
3.4.1.2	מקורות הרכשה והזנה אפשריים של טפסי טביעות אצבע (עמדות הטבעה, סריקת טפסים, מדיה חיצונית, ממשקים, זירות עבירה וכו').			
3.4.1.3	איתור ואימות זהות של אדם או מעתקים, על פי טביעות אצבע ממקורות שונים (ממשקים, רכיבים ניידים/ סלולאריים וכו'), מול המאגר, בדגש על הפונקציות הבאות:			
*	פונקציית TP-TP.			
*	פונקציית UL-TP.			
*	פונקציית LT-TP.			
*	פונקציית PL-TP.			
*	פונקציית LT-UL.			
*	פונקציית ULP-PP.			
*	פונקציית ULP-LP.			
*	פונקציית קידוד TP מתוך תמונה.			
*	אפשרות להגדרת קבוצה סגורה וביצוע החיפוש רק			

	מול קבוצה זו (Close search), בפונקציית: LT-TP , LP-PP , LP-ULP , TP-TP , LT-UL , UL-TP.			
3.4.1.4	פירוט ביצועים, זמני תגובה, רמת הדיוק של המערכת כפונקציה של שרתי החיפוש, יכולת העיבוד שלהם ואיכות דיוק האלגוריתם.			
3.4.1.5	פירוט יכולת האינטגרציה של המערכת עם מערכות חיצוניות, כולל פרוטוקולים נתמכים כמו SDK, API. החברה תפרט את ניסיונה במימוש ממשקים עם מערכות של גורמי אכיפת חוק בין - לאומיים.			
3.4.1.6	קידוד טביעת אצבע וכף יד מאדם מצילום תמונה שצולם במצלמה.			
3.4.1.7	תיעוד ורישום טביעות אצבע בשטח (טפסים ומעתקים), באמצעות רכיב נייד, ושליחתן למערכת המרכזית ממקורות שונים.			
3.4.1.8	צילום פני אנשים ושמירת התמונה כחלק מ-Metadata, יכולות עיבוד תמונה מתקדמות.			
3.4.1.9	פירוט הפונקציות לביצוע עיבוד, התאמה, פעולות ניתוח ועדכונים של טביעות אצבע ומעתקים, ע"י מומחה.			
3.4.1.10	פירוט ביצוע תהליך עבודה של מומחה שני על המסד, על פי תהליך ACE-V עיבוד המידע, לצורך הצגתו בבית המשפט (Charting).			
3.4.1.11	הפקת שאילתות ודו"חות - פירוט כל האפשרויות להפקת דוחות שונים במערכת, לרבות פירוט			

	יכולות באמצעות בינה מלאכותית (AI).			
3.4.1.12	ניהול המערכת - פירוט היכולות הקיימות בעמדת מנהל המערכת, יש להתייחס גם ליכולת להגדרת פרופילים והרשאות שונות למשתמשים השונים.			
3.4.1.13	הדרכה והטמעה - פירוט אמצעי ההדרכה והתרגול במערכת (עמדות, חומרה ותוכנה), לעמדות השונות ולמפעילים השונים.			
3.4.1.14	סביבת בדיקות - החברה תציג את הפתרון המוצע להקמת סביבת בדיקות למערכת.			
3.4.2	עמדות קצה			
3.4.2.1	המשתתף יספק מידע לפתרונות חומרה ותוכנה עבור עמדות הקצה המפורטות בסעיף 2.4 לעיל ועל עמדות קצה נוספות ככל שישנן בקשר למערכת נשוא המענה, בדגש על הנושאים הבאים:			
*	מפרט טכני למחשב , האם האפליקציה נתמכת בעמדות מחשב סטנדרטיות.			
*	מערכת הפעלה נתמכת, האם העמדה נתמכת בסביבת מיקרוסופט , מערכות הפעלה של מיקרוסופט וגירסאותיה .			
*	סוגי סורקי טי״א כולל תקנים נתמכים בדגש על תקן FBI.			
*	מצלמה ביומטרית (רזולוציה ותקנים נתמכים).			
*	יכולות AI.			
*	תמיכה במצב לא מקוון.			
*	יכולות הצפנה על נתונים ביומטריים בעמדה.			

*	בקרת כניסה והרשאות משתמשים.			
*	אופן הפצת עדכוני תוכנה.			
3.4.2.2	רכיבים ניידים – סורקי ט״א ומסופונים			
*	רכיב לזיהוי מהיר המיועד לאימות זהות או איתור זהות של אדם:			
*	פירוט על משטח הטבעה בדגש על גודלו הפיזי של הרכיב , גודל המשטח ורזולציה.			
*	המשתתף יתאר את הנתונים הטכניים של הרכיב והאם כולל API סטנדרטי לצורך פיתוח ממשקים ו- SDK לצורך פיתוח.			
*	אופן החיבור (USB סטנדרטי , (Type c ליחידת הקצה כגון מחשב, טאבלט.			
*	מערכות ההפעלה בהן הרכיב נתמך Windows android, וכד׳)			
*	האם הרכיב נתמך ב (Citrix) Terminal Server CITRIX			
3.4.2.3	מסופון /טאבלט נייד לזיהוי מהיר (Fast Id)			
*	המשתתף יתאר את הרכיב בדגש על הפונקציות הבאות:			
*	בדיקה מול מאגר מקומי (Wanted List) וגם מול מאגר המרכזי באמצעות תקשורת פנים משטרתית ותקשורת סלולארית .			
*	האם המסופון כולל קורא כרטיס חכם (Smart Card) מסוג contact / contactless.			

*	מערכת ההפעלה בה תומך המסופון.			
*	סוגי החיבורים במסופון.			
*	רמת האטימות בפני רטיבות ואבק			
*	עמידות לטמפרטורה גבוהה.			
*	פירוט יכולות הסוללה			
3.4.2.4	עמדה ניידת להרכשת ט״א מגופות			
*	פירוט על מערכת ניידת אשר תוכל לבצע נטילת ט״א ישירות מגופות וזיהוי הטביעות מול מאגר נייד ומול המאגר המרכזי.			
*	כולל כל הרכיבים הנדרשים לצורך ביצוע כל הפעולות הנדרשות להרכשת ט״א מגופות.			
3.4.2.5	רכיב נייד לצילום ט״א בזירת עבירה			
3.4.3	הסבת נתונים			
3.4.3.1	תיאור יכולות הסבת הנתונים ותהליך ביצוע ההסבה ממערכת קיימת למערכת נשוא המענה, בדגש על המאגרים הבאים:			
3.4.3.1.1	מאגר ט״א וכפות ידיים ממקורות שונים, אשר עברו עיבוד במהלך קליטתן ושמירתן במערכת.			
3.4.3.1.2	מאגר מעתקי ט״א וכפות ידיים, אשר עברו עיבוד במהלך קליטתם ושמירתם במערכת.			
3.4.3.2	יכולות טיוב המאגרים במהלך ההסבה.			
3.4.3.3	יכולות שימוש ב- AI בתהליך הסבת הנתונים.			
3.4.3.4	ההכנה הנדרשת מספק המערכת המוסבת לצורך ההסבה.			
3.4.3.5	על החברה לפרט את ניסיונה בהסבת נתונים של			

	מערכת הכוללת לפחות 3,000,000 טפסי ט״א ו- 250,000 מעתקי ט״א, בדגש על הפרמטרים הבאים:			
3.4.3.5.1	פרטי הלקוחות ואנשי קשר בלקוח (במידה של חובת חסיון - נא לפרט את סוג הלקוח ומידע כללי).			
3.4.3.5.2	יצרן המערכת ממנה הוסבו הנתונים.			
3.4.3.5.3	סוג בסיס הנתונים.			
3.4.3.5.4	משך הזמן בו התבצעה ההסבה.			
3.4.3.5.5	אופן המעבר בין המערכת הישנה לחדשה, תוך התייחסות לרציפות תפקודית.			
3.4.4	אבטחת מידע והגנת סייבר			
3.4.4.1	פירוט תקני אבטחת מידע והגנת הסייבר שהארגון והמערכת עומדים בהם, כגון NIST, ISO, SOC2, GDPR וכדי.			
3.4.4.2	בקרות אבטחת המידע והגנת הסייבר אשר בשימוש המערכת/השירות.			
3.4.4.3	אופן שילוב תהליך SDLC במחזור חיי המערכת/השירות כולל בדיקות תוכנה.			
3.4.4.4	במידה והמשתתף מציע שימוש בתשתית מחשוב של ספק אחר, עליו לציין זאת ולצרף מסמך המתאר כיצד מתבצעת חלוקת האחריות בינו לבין ספק התשתית הנוסף ובאילו אמצעים הוא נוקט בכדי להגן על המידע מפני פגיעות ברמת התשתית.			
3.4.4.5	פירוט יישום ואופן התמיכה במערכות ניטור ובקרה, בהעברת קבצי לוג ואירועים למערכות			

	אוטומציה וניטור אבטחתי כגון SIEM ו- SOAR כגון SYSLOG.			
3.4.4.6	פירוט תמיכת המערכת במנגנוני הזדהות כדוגמת SSO, IAM.			
3.4.4.7	פירוט האם המערכת מכילה אפשרות לבדיקה ביומטרית כהרשאה לכניסה למערכת.			
3.4.4.8	פירוט לגבי תמיכת המערכת בהחלת מדיניות החלפת סיסמאות, אשר תכלול קביעה של משתנים כגון: אורך, מורכבות, תוקף, היסטוריה, אכיפת MFA וכדומה.			
3.4.4.9	פירוט אופן תמיכת המערכת בהרשאות גישה מצומצמות ככל האפשר (Least Privilege) לביצוע פעולות מורשות למשתמשי המערכת, בכדי להגן על הנתונים מפני גישה לא מורשית, חשיפה, שיבוש, שינוי או מחיקה.			
3.4.4.10	פירוט כלל פרוטוקולי ההצפנה הקיימים במערכת (לרבות סוג ההצפנה לדוגמה AES 256bit וגודל מפתח לדוגמה 2048 ומעלה), עבור הצפנת המידע והתקשורת מקצה לקצה, הצפנת המידע הן בתנועה ובמנוחה.			
3.4.4.11	פירוט תמיכת המערכת בשמירת מפתחות ההצפנה במערכות אבטחת חומרה(HSM) ושירותי ניהול מפתח (KMS) ו/או בכל פתרון אחר המספק הגנה על המפתחות. על החברה לפרט כיצד מיושם מענה זה.החברה תפרט כל מידע נוסף שנוגע לאבטחת מידע והגנת הסייבר הקשור למערכת.			

3.4.5	תשתיות המערכת			
3.4.5.1	מידע על דרישות החומרה, מערכת ההפעלה ותשתיות רשת נדרשות.			
3.4.5.2	מענה התקשורתי לעבודה בתצורת ACTIVE- ACTIVE לרבות הגדרת קבצי תעבורה נדרשים בין האתרים.			
3.4.5.3	נפח וקצב העברת המידע של הקבצים ואת רוחב הסרט המינימאלי המאפשר עבודה תקינה. יצוין כי החברה תידרש לעבוד על בסיס התשתית האקטיבית הקיימת במשטרת ישראל.			
3.4.5.4	על החברה לפרט את אופן המענה - פתרון WEB / התקנת תוכנה מקומית (קליינט) / CITRIX.			
3.4.5.5	מצב של ניתוק תקשורת בין הליבה לתחנות הקצה.			
3.4.5.6	דרישות הציוד הנדרשות ליישום הפתרון (קצה/ היקפי/ תוכנה).			
3.4.5.7	האם יש אפשרות לעבודה על בסיס טכנולוגית מחשוב מרוחק - citrix xenapp/xendesktop גרסאות 7.15 ומעלה? האם יש אפשרות לעבודה בסביבת מחשוב מרוחק בתצורת Terminal Server? האם ההתקנים הפריפריאליים יכולים לעבוד בתאימות לתצורת Citrix XenApp? ה-			
3.4.5.8	האם תיתכן התממשקות למערכות הארגון באמצעות API.			
3.4.5.9	כיצד מתוכנן היישום כך שיפעל היטב בסביבת			

	משאבים משותפים, ללא גרימת הפרעה ליישומים האחרים הפועלים על אותו שרת.			
3.4.5.10	מהן מערכות ההפעלה בהן נעשה שימוש			
3.4.5.11	מהם מסדי הנתונים שבשימוש המערכת.			
3.4.5.12	על האם המוצר המוצע להיות מסוגל לפעולנתמך בסביבות Microsoft Windows סטנדרטיות עתידיות. יש לתאר במענה סביבות נוספות אשר המוצר מתאים עבורן, אם קיימות.			
3.4.5.13	משטרת ישראל מקיימת סטנדרט ארגוני בכל הקשור ברכש שרתים. החברה תפרט האם היישום יכול להיות מותקן על גבי תשתית משטרתית? מה הם המשאבים הנדרשים לכך? במידה ולא - נדרש לפרט מה נדרש חומרתית ואפליקטיבית ע"מ ליישם את האפליקציה.			
3.4.5.14	שרתים - מערך השרתים במשטרת ישראל תומך ב High Availability וב- בתשתית וירטואלית מבוססת vmware. בהקבלה למשטרת ישראל, כיצד נבנה מערך השרתים ביישום הזה?			
3.4.5.15	מה היא תצורת העבודה הפיזית המינימלית מבחינת כוח עיבוד, זיכרון ועוד (עבור השרתים).			
3.4.5.16	שיטת ההפעלה. האם תתקיים בתצורת stretch site ע"י הפעלת היישום בשגרה בשני האתרים בו זמנית תוך חלוקת עומסים (בתצורת Active\Active) או בתצורה אחרת? האם			

	קיימת יכולת התחברות ל-2 האתרים במקביל בתצורת רשת של ? Layer2 over layer3			
3.4.5.17	האם תיתכן עבודה בשני אתרים במקביל. מהן יכולות הסנכרון בין שני האתרים?			
3.4.5.18	האם קיים איזון עומסים? F5 Gslb?			
3.4.5.19	כיצד המערכת תומכת בפתרונות שרידות והמשכיות של השירות גם במקרה תקלה. האם קיימת שרידות ויתירות בכל רכיבי התשתית כולל מכונות האחסון ומתגי התקשורת? (נדרש לפרט).			
3.4.5.20	כיצד מתבצע תהליך אחסון נתונים וע"י איזה חברה. האם תתאפשר שמירה מרכזית במכונות אחסון מבוססות בטכנולוגיה SAN של חברת Hitachi המחוברות למתגי אחסון העובדים בטכנולוגיה SAN של Brocade?			
3.4.5.21	מה הן תחנות העבודה ומה כוח העיבוד בהן.			
3.4.5.22	מערך השו"ב הנלווה - כיצד מתבצע תהליך ניטור רכיבי תשתית? האם תתכן שימוש במוצרי Microsoft SCOM 2012 ו- Zabbix.			
3.4.5.23	האם ניתן להגדיר Key Performance Indicators (KPI).			
3.4.5.24	האם קיים ניטור רכיבים אפליקטיביים וכן האם המערכת תתמוך בשליחת התרעות למערכת שו"ב ע"י SNMP או ע"י הפעלת כלי			

	התראה נוספים (exe, dll או Web Service) .			
3.4.5.25	פירוט אודות מערך הגיבוי ותוכנת הגיבוי בהם נעשה שימוש. האם תתאפשר תמיכה בגיבוי Snap של תשתית וירטואלית?			
3.4.5.26	סביבת המחשוב המשטרתית הינה סביבה סגורה שאינה מאפשרת קישור לאינטרנט או לרשת תקשורת חיצונית אחרת. האם נדרש חיבור לאינטרנט לצורך הפעלת התוכנה?			
3.4.5.27	כיצד מתבצע הגיבוי של המערכת? מה התוכנה בה משתמשים			
3.4.6	שירותי תמיכה ותחזוקה			
3.4.6.1	פרטים אודות מחזור חיים צפוי של המערכת, כולל משך הזמן שבו תתפקד ללא צורך בשדרוג משמעותי וכן תכניות לשדרוגים עתידיים.			
3.4.6.2	סוג התמיכה הטכנית הנדרשת למערכת.			
3.4.6.3	מדיניות היצרן בנוגע להפצת גרסאות, תת-גרסאות ועדכונים.			

משטרת ישראל

נספח ד'

טבלת ניקוד - מעבר לשלב ההדגמה

סעיף ב-RFI	תמצית/כותרת	ניקוד מקסימלי	ציון	נדרש
5.8.1.2.1	המשתתף הוא יצרן המערכת נשוא המענה או נציגות מורשית של היצרן (דרישת חובה).	15		המצאת אישור
5.8.1.2.2	המערכת בעלת תקן למערכות טביעות אצבע בתחום האפיס הפלילי (דרישת חובה).	10		המצאת אישור
5.8.1.2.3	מערכת AFIS פלילי של היצרן נבחנה במהלך 3 השנים האחרונות לפחות במבדק דיוק אחד שנערך ע"י אחד או יותר מארגוני התקנים הבינלאומיים (דוגמת FBI, ANSI/NIST) (דרישת חובה).	10		המצאת אישור
5.8.1.2.4	המערכת בעלת תקן אבטחת מידע והגנת הסייבר, כגון: NIST, ISO, SOC2, GDPR (דרישת חובה).	10		המצאת אישור
5.8.1.2.5	ליצרן המערכת ניסיון של 5 שנים לפחות (2020-2024 כולל), בייצור, התקנה, הפעלה ותחזוקה של מערכות AFIS פלילי (דרישת חובה).	15		המצאת אישור
5.8.1.2.6	ליצרן לקוחות שונים אצלם הותקנה מערכת אפיס פלילי ולהם הוא מספק שירותי אחזקה מלאה ב-5 השנים האחרונות לפחות (נקודה לכל לקוח, מקס' 10 נק')	10		המצאת אישור
5.8.1.2.7	היצרן סיפק והתקין 3 מערכות אפיס פלילי במדינות האיחוד האירופאי ו/או בארה"ב ו/או בקנדה ו/או באוסטרליה ו/או בניו-זילנד (5 נקודות לכל מערכת, מקס' 15 נק')	15		המצאת אישור
5.8.1.2.8	ליצרן לפחות 3 לקוחות אצלם מותקנת מערכת אפיס פלילי הכוללת מאגר של לפחות 4,000,000 רשומות טביעות אצבעות (5 נקודות לכל לקוח, מקס' 15 נק')	15		המצאת אישור

משטרת ישראל

לכבוד **נספח ה'**

מדינת ישראל - משטרת ישראל
המטה הארצי רמלה, רח' בעלי המלאכה 41

א.ג.נ.,

נספח ביטוח כללי להסכם ההתקשרות

המשתתף מתחייב לערוך ולקיים ביטוחים הולמים ביחס לשירותים ו/או העבודות נשוא הסכם זה עבור מדינת ישראל – משטרת ישראל (להלן: "המזמין"), ככל שנהוגים בתחום פעילותו (לדוגמה: ביטוח חבות מעבידים, ביטוח אחריות כלפי צד שלישי, ביטוח אחריות מקצועית, ביטוח חבות מוצר, ביטוח עבודות קבלניות, ביטוח משולב אחריות מקצועית/מוצר, ביטוח צמ"ה, ביטוח רכוש, ביטוח סחורה בהעברה או כל ביטוח אחר, לפי העניין), בגבולות אחריות סבירים בהתאם לאופיים והיקפם של השירותים ו/או העבודות נשוא הסכם זה. ככל ויועסקו ע"י המשתתף קבלני משנה, עליו לוודא שביטוחיו כוללים כיסוי לאחריותו בגינם, וכן לדרוש מהם לערוך ביטוחים לכיסוי אחריותם הישירה, כנדרש בנספח זה. כחלופה, המשתתף יוודא כי ביטוחיו יכללו כיסוי לפעילותו ולאחריותו הישירה.

המשתתף יוודא כי בכל הביטוחים שערך לפי נספח זה (למעט ביטוח מסוג עבודות קבלניות/הקמה), המזמין יתווסף כמבוטח נוסף בכפוף להרחבת שיפוי כמקובל באותו סוג ביטוח.

המשתתף יוודא כי בביטוח מסוג עבודות קבלניות/הקמה, ככל ונערך ביחס לשירותים ו/או העבודות נשוא הסכם זה, ייכלל המזמין וכן כל הקבלנים וקבלני המשנה, כמבוטחים נוספים.

המשתתף יוודא כי בכל הביטוחים שערך לפי נספח זה, ייכלל סעיף ויתור על זכות התחלוף/השיבוב כלפי המזמין ועובדיו (ויתור כאמור לא יחול לטובת האדם שגרם את הנזק בזדון) וכן סעיף לפיו הביטוחים יהיו קודמים וראשוניים ללא זכות השתתפות ו/או חזרה.

למען הסר ספק מובהר, כי המשתתף אחראי בלעדית כלפי המבטח לתשלום דמי הביטוח, ההשתתפויות העצמיות עבור כל הפוליסות ולמילוי כל החובות המוטלות על המבוטח על פי תנאי הפוליסות.

משטרת ישראל שומרת לעצמה את הזכות לקבל מהמשתתף אישור על קיום ביטוח או העתקי פוליסות, מעת לעת ולפי דרישה.

אי עמידה בתנאי נספח זה מהווה הפרה של הסכם זה.

תאריך	**שם המשתתף (פרטי + משפחה)**	**חתימה וחותמת המשתתף**