אל: ועדת המכרזים

משרד:	משרד ראש הממשלה
יחידה מזמינה:	ממשל זמין
תאריך:	05.11.2020

הנדון: <u>חוות דעת מקצועית במסגרת כוונה להתקשר עם ספק יחיד/ ספק חוץ</u>

הבקשה מסתמכת על תקנה ☒ 3(29) / ☐ 3(31) לתקנות חובת מכרזים ועל הוראות תכ"ם מס' 7.8.1 ו-7.8.2.

תיאור מהות ההתקשרות (רקע ופירוט התכונות של הטובין/השירות/העבודה)

<u>רקע:</u>

ב 2015 ביצעה יחידת ממשל זמין רכש לתוכנת Splunk. בשנת 2017 הורחבה ההתקשרות מול הספק על מנת לממש אופציה של הגדלת נפח. כעת מבקשת היחידה להמשיך את ההתקשרות לצורך המשך קבלת תחזוקה עבור מוצר זה וכן המשך רכש רישיונות בשל גידול בנפחי הנתונים.

התקנת המוצר הייתה תהליך ארוך ומתמשך אשר החל לפני כ- 5 שנים. במהלך השנים, הוכנס המוצר כתשתית **SIEM** חדשה אשר החליפה את תשתית ה **SIEM** הישנה **Arcsight** . לצורך הטמעת המוצר ושיפור היכולות, הושקעו (ועדיין מושקעים בו) אלפי שעות אדם של אנשי ממשל זמין ויועצים חיצוניים, ובכלל זה 3 חברי צוות במשרה מלאה.

ככלל, למערכות **SIEM** אורך חיים כמעט בלתי מוגבל, אולם מאחר ו **Arcsight** הפסיקה להתקדם מבחינה טכנולוגית, נדרש ממשל זמין למצוא מוצר חלופי. היחידה בחנה במשך כ-3 שנים מוצרים חלופיים, עד שאיתרה את **Splunk** והחלה בהטמעה לפני כ-5 שנים.

מוצר ה **Splunk** מוגדר כיום כמוצר ליבה, מוצר קריטי בחשיבותו, המותקן בכלל סביבות העבודה של יחידת ממשל זמין.

<u>נכון להיום נוספו מקורות מידע חדשים בעקבות הגדילה הטבעית של יחידת ממשל זמין ולכן יש צורך להגדיל את יכולות העיבוד בכדי לענות לגדילה הטבעית של הארגון.</u>

היחידה מעוניינת להמשיך את ההתקשרות עם הספק על מנת לעשות שימוש במוצר. הספק היחיד אשר ניתן לקבל ממנו שירותים מקצועיים בהתאם לנדרש הינו חברת אמת מחשוב בע"מ, מהנימוקים המפורטים להלן:

<u>תיאור המוצר, תפקידו במערך ממשל זמין וייחודו</u>

1. מוצר Splunk הינו פלטפורמת ניטור וניתוח Big Data מהמובילות בעולם. המוצר משמש כ- Security Information and Event Management - SIEM ומספק דרך קלה, מהירה ובטוחה לנתח את זרמי הנתונים המסיביים שמפיקות מערכות המחשוב והתשתיות הטכנולוגיות בממשל זמין. המוצר אוסף את כל נתוני המערכות כדי לסייע בטיפול בתקלות, לחקירת אירועי סייבר תוך דקות במקום שעות או ימים ומאפשר לנתח את המידע תוך פרקי זמן קצרים, להתריע על אירועי אבטחה ואנומליות בכלל תשתיות ממשל זמין ולאפשר מתן תגובות יזומות. בכך מתמודדת היחידה עם אירועי אבטחת מידע בצורה מיידית ומיטבית.
2. מוצר ה Splunk מנטר באמצעות חיבור על ידי סוכן (Agent) למערכות רבות (באמצעות ממשק מכל מערכת). סך הכל מחוברות למערכת כ-1,800 (!) סוכנים ממערכות שונות (כ- 3,000 מקורות מידע). בנוסף, מעבר להתקנה הראשית של המוצר, ישנן התקנות נוספות בסביבת מסווגות של היחידה.
3. המוצר משרת את **כלל** המערכים בממשל זמין, לרבות אבטחת מידע BI, IT ועוד ומנטר את מערכות ותשתיות ממשל זמין. המוצר מספק נראות בזמן אמת ותובנות קריטיות לגבי חוויית הלקוח, טרנזקציות ומדדים חשובים אחרים ומאפשר להפוך את הנתונים לנגישים, שמישים ובעלי ערך בחלקי הארגון השונים.
4. המערכת מקבלת בממוצע 27,000 אירועים בשנייה.
5. במערכת קטלוג של כ-100 מיליארד אירועים, מתחילת חיי המערכת.
6. המערכת מאנדקסת כ TB1.8 ליום!
7. המערכת מוציאה כ 3,000 התראות מותאמות (לעובדי ממשל זמין ומשרדי ממשלה אחרים) ביום.
8. היות וייחודו של מוצר SIEM הינו לתת באמצעות שולחן פיקוד (Dashboard) תמונה מקיפה וכוללת של מצב אבטחת המידע בכלל המערכות והתשתיות, תוך התרעה על אירועים ואנומליות שונות המתגלות. אין אפשרות בשלב זה להוציא את המוצר משימוש בממשל זמין ולהחליפו במוצר אחר. יתרה מזו, לא ניתן לשלב את המוצר עם מוצר נוסף, היות ונדרש ריכוז של כלל המידע במקום אחד.
9. מדובר על מוצר מהותי שרמת האינטגרציה שלו למערכות השונות היא מורכבת מאוד. משך החיים של מוצרים מסוג זה הוא בדרך כלל יותר מעשר שנים. בנוסף, חלק מחוזקו של המוצר הינו ביכולות האנליטיקה על גבי מחסן מידע גדול לנושאי אבטחה. חוזק זה נבנה רק כאשר המוצר מוטמע לאורך זמן. הטמעה של מוצר SIEM הינה בהיקף של כמה שנות אדם, והחלפה של מוצר כזה לאחר שנים ספורות תדרוש השקעות רבות מיותרות.
10. מוצרים אחרים מנסים לקרוא תיגר על Splunk . אנחנו עמלים, **באופן רציף**, בבדיקת השוק ובבחינת חלופות. נכון להיום, לא מצאה היחידה מוצר שיכול להחליפו, לא מבחינת רמת הטכנולוגיה ולא מבחינת רמת התפעול.

11. ההתקשרות המבוקשת תאפשר לנו המשך של תחזוקת המוצר בגין נפחי נתונים המערכות הקיימים, רכישת רישיונות נוספים עבור נפחי נתונים ההולכים וגדלים וכן רכישת שירותים מקצועיים בהתאם לציוד המותקן בחוות השרתים בממשל זמין, תוך השתלבות במערך הקיים של מוצרים מתוצרת זו הכוללים מרכיבי חומרה, תוכנה וניהול וממשקים לכלל מערכות ממשל זמין, עם יכולת התאמה למימוש מדיניות האבטחה של ממשל זמין.

האם קיים בנושא ההתקשרות מכרז חשכ"לי ☐ כן ☒ לא

סוג ההתקשרות: (סמן **X** במקום המתאים)

☒ טובין ☒ שירותים

שם הספק:	**אמת מחשוב** בע"מ	
מספר הספק (ח.פ/ח.צ/ע.מ/מספר עמותה)	ח.פ 520038514	
ספק זה הנו:	☒ ספק יחיד	☐ ספק חוץ
אומדן / שווי ההתקשרות:	רכש רישיונות (כ- 3,200,000₪) ושירותים מקצועיים (כ- 600,000₪): סה"כ 3,800,000 ₪ כולל מע"מ	
תקופת ההתקשרות:	31.12.2021-31.12.2020	

נימוקים כי הספק הוא ספק יחיד או כי הטובין הם טובי חוץ

חברת אמת מחשוב בע"מ, הייתה הספק היחיד אשר הוגדר כשותף ברמת ELITE של חברת Splunk ולכן עד כה יחידת ממשל זמין רכשה רישוי ותחזוקה מספק זה בלבד, בהתאם להליך ספק יחיד.

החל **מאוקטובר 2020**, הוגדרה גם חברת מטריקס כשותפה ברמת ELITE של חברת Splunk. בשלב בו הוגדרה חברת מטריקס כשותפה, כבר היתה היחידה המקצועית בשלבים אחרונים של הגשת כל מסמכי ספק יחיד לוועדת המכרזים (כבשנה שעברה).

למרות האמור לעיל, מבירור מול חברת Splunk ,הובהר ליחידה כי אמת מחשוב היא החברה **היחידה** בארץ המוסמכת ע"י היצרן להטמעה וליווי של פרויקטים, כפי שמופיע באתר היצרן: Professional Services specialization: Core implementation. שירות זה הינו קריטי לתפעול המערכת בממשל זמין.

בנוסף - לאור הצורך ההולך וגובר בעיבוד מידע והצגתו בממשל זמין (עבור כל היחידה והן עבור משרדי הממשלה), היחידה נדרשת לידע תפעולי רב בפעילות השוטפת. ה Roadmap העתידי (והמצב העכשווי) מחייב את ההסמכות הבאות:

- Splunk Core Certified Consultant
- Splunk Enterprise Certified Architect
- Splunk Enterprise Certified Admin
- Splunk IT Service Intelligence Certified Admin
- Splunk Accredited Implementation Fundamentals

מאחר ואמת מחשוב בע"מ, הינו הספק היחיד אשר מוגדר כשותף של חברת Splunk ברמת ELITE, אין לאף ספק אחר, **בזמן הנוכחי**, מלבד אמת מחשוב, את הידע והיכולת הנדרשת - רמת ידע ויתירות זו חיונית להתקשרות לציוד כה קריטי לפעולתו התקינה של ממשל זמין.

לאור האמור לעיל, אמת מחשוב הינה החברה היחידה איתה ניתן להתקשר בעת הזו.

3. נימוקים והערות נוספות

לאור דינמיות השוק, יתכן כי בעתיד יוכלו שותפים נוספים לספק שירותים מקצועיים (Professional services) ברמה הנדרשת ועל ידי המומחים הנדרשים. לכן אנו מבקשים כי הספק יחיד לצורך רכש הרישיונות לאור ההצעה המיטיבה, יהיה לתקופה של שנה.

<u>סיכום</u>

לאור הצורך כפי שפורט לעיל, אנו מבקשים אישור להגדיר את חברת אמת מחשוב בע"מ כספק יחיד לצורך הספקת מוצרי Splunk ושירותים מקצועיים למשך תקופה של שנה אחת, תוך בחינת מצב השוק ורמת השותפים במתן שירותים מקצועיים ובמידת הצורך קיום מכרז לרכש מוצרי Splunk ושירותים מקצועיים בהתאם.

חוות דעתי זו ניתנת מתוקף היותי הסמכות המקצועית לנושא זה.

בכבוד רב,

חגי פרלמוטר	מנהל מערך הגנה בסייבר	
שם בעל הסמכות המקצועית	**תפקיד בעל הסמכות המקצועית**	**חתימה**

יוגב שמני	מנהל ממשל זמין	
שם בעל הסמכות המקצועית	**תפקיד בעל הסמכות המקצועית**	**חתימה**