

שם הטופס: חוות דעת מקצועית במסגרת כוונה להתקשר עם ספק יחיד/ספק חוץ	
פרק ראשי: התקשרויות ורכישות	מספר הוראה: 7.8.2
פרק משני: פטור ממכרז	מספר טופס: ט. 7.8.2.1

משרד:	
יחידה מזמינה:	
תאריך:	

אל: ועדת המכרזים



הנדון: חוות דעת מקצועית במסגרת כוונה להתקשר עם ספק יחיד/ ספק חוץ רכישת מנוי שנתי לעדכון חתימות מערכת זיהוי חתימות של ממשל זמין.

הבקשה מסתמכת על תקנה 3(29) / 3(31) (סמן את התקנה המתאימה) 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)
 מערך אבטחת המידע בממשל זמין מפעיל שכבות רבות בהגנה על מערכות המידע והאתרים השמורים בשרתים שלו. אמצעי קריטי כזה הוא מערכת זיהוי מתקפות (IDS) מסוג Snort המבוססת קוד פתוח. מערכת זו מכילה אמצעים לזיהוי אלפי סוגי ההתקפות המצויות בעולם והמופנות מידי יום לשרתי ממשל זמין. זיהוי של התקפה על פי התנהגותה נקרא 'חתימה'. מידי יום, כמענה על התקפות חדשות, נוצרות חתימות חדשות שיש לעדכן במערכת. מערכת זו זקוקה לשדרוג, תמיכה ועדכוני חתימות על בסיס יומיומי, אשר אותם מספקת לנו חברת Sourcefire האמריקאית שהיא הבעלים של מוצר ה SNORT

האם קיים בנושא זה מכרז מרכזי של החשב הכללי או גורם ממשלתי מוסמך אחר? כן לא
 סוג ההתקשרות: (סמן X במקום המתאים)

טובין שירותים ביצוע עבודה

שם הספק:	SourceFire.com
מספר הספק (ח.פ./ח.צ.ע.מ./מספר עמותה)	 SF Bank Detail-1.pdf מצורף פרטי חשבון בנק
ספק זה הנו:	<input checked="" type="checkbox"/> ספק יחיד <input checked="" type="checkbox"/> ספק חוץ
אומדן / שווי ההתקשרות:	 Tehilia_VRT_Quote.p df, 20,000 ₪, מצורפת הצעת מחיר,
תקופת ההתקשרות:	

שם הטופס: חוות דעת מקצועית במסגרת כוונה להתקשר עם ספק יחיד/ספק חוץ

פרק ראשי: התקשרויות ורכישות	מספר הוראה: 7.8.2
פרק משני: פטור ממכרז	מספר טופס: ט. 7.8.2.1

נימוקים כי הספק הוא ספק יחיד או כי הטובין הם טובי חוץ
(במקרה הצורך ניתן לצרף עמודים נוספים וכל מסמך רלוונטי נוסף)


מערכת Snort היא המערכת הקיימת בתהיל"ה ומכילה סנסורים שונים האוספים מידע על מתקפות באמצעות ניטור תעבורה והחשדה של פעולות חריגות מול רשת תהיל"ה. חיוני כי אמצעי הזהיו של המתקפות השונות (חתימות) תהיינה עדכניות ברמה יזמית עקב המספר הרב של סוגי ההתקפות וההתפתחות המתמדת של התוקפים השונים. לצורך פעולתה התקינה של המערכת אלטרנטיבות שנבחנו:

א. החלפת מערכת ה SNORT במערכת אחרת: פעולה כזו היא פעולה אסטרטגית המחייבת היערכות טכנולוגית, מנהלתית וכלכלית. ההשלכות שלה רחבות מאוד ולא נותחו. פעולה כזו לא מצויה בתכנית העבודה 2012.

ב. אי-עדכון המערכת: אי-עדכון המערכת יגביר משמעותית את הסיכונים למערכות המידע של תהילה עד כדי סיכון מהותי לחדירה והשבתה.

חוות דעתי זו ניתנת מתוקף היותי הסמכות המקצועית לנושא זה.

בכבוד רב,

שוקי פלג	מנהל אבטחת מידע – ממשל זמין	
שם בעל הסמכות המקצועית	תפקיד בעל הסמכות המקצועית	חתימה