רשומות

הצעות חוק

ה ממ ש ל ה

י"ט בתמוז התשפ"ה | 1888 | 15 ביולי 2025

עמוד

הצעת חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה – חרבות ברזל) (תיקון מס' 3), התשפ"ה–2025 984

הצעת חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה – חרבות ברזל) (תיקון מס׳ 3), התשפ״ה–2025

תיקון שם החוק

1. בחוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה – חרבות ברזל), התשפ״ד–2023[1] (להלן – החוק העיקרי), בשם החוק, במקום ״(הוראת שעה – חרבות ברזל)״ יבוא ״(הוראת שעה)״.

דברי הסבר

כללי מתחילת הלחימה במסגרת מבצע ״חרבות ברזל״ (להלן – חרבות ברזל), ביום כ״ב בתשרי התשפ״ד (7 באוקטובר 2023), ניכרת עלייה בהיקף ובעוצמה של תקיפות סייבר נגד גופים אזרחיים במשק הישראלי. מטרת תקיפות סייבר אלה היא לפגוע, כחלק מהמתקפה המשולבת המכוונת כלפי חוסנה של מדינת ישראל, במרחב הסייבר הישראלי, בכלכלה ובתפקודו התקין של המשק הישראלי, והן אף עשויות להביא לפגיעה בחיי אדם. תקיפות הסייבר, לפי עמדת גורמי המקצוע במערך הסייבר הלאומי, בשירות הביטחון הכללי (להלן – שב״כ) וביממונה על הביטחון במערכת הביטחון (להלן – מלמ״ב), הולכות והופכות מתוחכמות ומורכבות יותר.

ספקים רבים של שירותי אחסון ושל שירותים דיגיטליים מתאפיינים בחיבוריות גבוהה לגופים רבים במשק הישראלי, לרבות למשרדי ממשלה וגופים ציבוריים, ובהם גם גופים ביטחוניים, תשתיות מדינה קריטיות וארגונים חיוניים לתפקודו של המשק, ועוד. בשל חיבוריות זו, הנזק שעשוי להיגרם מתקיפה כנגד ספקים אלה עלול להתפשט ולהשפיע על חברות רבות במשק, ולכן פעמים רבות מהווים הם יעד מועדף לתקיפות סייבר. בשים לב לאמור, תקיפות סייבר חמורות כנגד ספקים אלה עלולות להביא לפגיעה בביטחון המדינה, בביטחון הציבור או לפגיעה חמורה ברציפות אספקתם של שירותים חיוניים לציבור.

כדי להתמודד עם הצורך המתואר לעיל, התקינה הממשלה, ביום י״ד בכסלו התשפ״ד (27 בנובמבר 2023), את תקנות שעת חירום (חרבות ברזל) (התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון), התשפ״ד–2023 (להלן – תקנות שעת החירום הראשונות), ובסמוך לאחר מכן, ביום י״ד בטבת התשפ״ד (26 בדצמבר 2023) פורסם ברשומות חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה – חרבות ברזל), התשפ״ד–2023 (להלן – החוק), אשר החליף את תקנות שעת החירום הראשונות. יצוין כי החוק נחקק למשך שבעה חודשים מיום פרסומו, והוארך פעמיים בחוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה – חרבות ברזל) (תיקון), התשפ״ד–2024, מיום י״ז בתמוז התשפ״ד (23 ביולי 2024), וכן בחוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה – חרבות ברזל) (תיקון מס׳ 2), התשפ״ה–2025, מיום ב׳ בניסן התשפ״ה (31 במרץ 2025), כך שהוא עומד בתוקף עד יום כ״ו בחשוון התשפ״ו (17 בנובמבר 2025).

החוק, בנוסחו כיום, מסמיך מנהל מוסמך בשב״כ ובמלמ״ב (להלן – הגופים), וכן את ראש חטיבת ההגנה בסייבר בצה״ל, לקבוע כי תקיפת סייבר היא תקיפת סייבר חמורה, אם יש חשש ממשי שיש בה כדי לפגוע בביטחון המדינה, בביטחון הציבור או בקיום האספקה והשירותים החיוניים; ובהמשך לכך – נתונה לעובד מוסמך באחד הגופים הסמכות להורות לספק על קיומו של חשש לתקיפת סייבר חמורה כנגדו. אם הספק לא הגיש תצהיר לפי החוק, וכן לא פעל באופן הולם ובתוך פרק זמן סביר שניתן לו לטיפול בתקיפת הסייבר החמורה, מסמיך החוק את העובד המוסמך לתת לספק הנתקף הוראות לצורך איתור התקיפה, מניעתה או בלימתה, תוך שהחוק קובע תנאים למתן ההוראות כאמור.

ביום י״ז בסיוון התשפ״ה (13 ביוני 2025) החלה המערכה מול איראן, במסגרת מבצע ״עם כלביא״, וזאת בעקבות החלטתה מאותו היום של ועדת השרים לענייני ביטחון לאומי על נקיטת פעולות צבאיות משמעותיות לפי סעיף 40 לחוק־יסוד: הממשלה. לנוכח המערכה נגד איראן והערכת הגופים באשר לחומרת איומי הסייבר והסיכונים הנשקפים מהם, ועל רקע הצורך המבצעי הדחוף בהקניית סמכויות וכלים חיוניים נוספים לשם התמודדות עם אותם איומים, הותקנו ביום כ״ז בסיוון התשפ״ה (23 ביוני 2025) תקנות שעת חירום (חרבות ברזל) (סמכויות נוספות לשם התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון), התשפ״ה–2025 (להלן – תקנות שעת החירום השניות). תוקפן של תקנות אלה נקבע עד יום כ״ז בתמוז התשפ״ה (23 ביולי 2025) והן קובעות, בין השאר, כי אם היה יסוד סביר למנהל המוסמך להניח כי תקיפת סייבר שמתרחשת או שיש חשש ממשי כי היא עומדת להתרחש, היא תקיפת סייבר חמורה, הוא רשאי לדרוש מהספק להציג לו כל ידיעה או מסמך אם הם נדרשים לשם בחינת התקיימותם של התנאים לקביעה כי תקיפת סייבר היא תקיפת סייבר חמורה. נוסף על כך, נקבע

[1] ס״ח התשפ״ד, עמ׳ 410; התשפ״ה, עמ׳ 426.

תיקון סעיף 1

2. בסעיף 1 לחוק העיקרי –

(1) לפני ההגדרה "חומר מחשב", "מחשב", "פלט" ו"תוכנה" יבוא:

"ארגון מקושר" – ארגון שקיים חיבור, פיזי או לוגי, קבוע או עיתי, בין מחשביו לבין מחשבי הספק, או שמתבצעת העברת חומר מחשב, קבועה או עיתית, בין מחשבי הספק למחשביו;";

דברי הסבר

בתקנות שעת החירום השניות כי אם לספק נודע על תקיפת סייבר משמעותית נגדו עליו לדווח באופן מיידי למנהל המוסמך, וכן חובה על ספק הנתקף בתקיפת סייבר חמורה ליידע בלא דיחוי כל ארגון מקושר אשר עלול להיפגע מן התקיפה באופן ישיר וממשי.

לנוכח הערכות מקצועיות של הגופים באשר לחומרת איומי הסייבר העדכניים והסיכונים הנשקפים מהם, ולנוכח מאפייניו הייחודיים של מרחב הסייבר, עמדת הגופים היא כי יש צורך לשמר את הסמכויות והכלים הנדרשים לצורך התמודדות עם תקיפות במרחב הסייבר. לפיכך, הסמכויות והכלים החיוניים, אשר נקבעו בעיקרם במסגרת החוק ותקנות שעת החירום השניות, לצורך התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון, נדרשים לשם שמירה על ביטחון המדינה, ביטחון הציבור ומניעת פגיעה חמורה ברציפות אספקתם של שירותים חיוניים לציבור. זאת, אף במנותק מן הלחימה במסגרת חרבות ברזל ומהמערכה מול איראן.

לכן, מוצע להוסיף לחוק את הסמכויות והכלים שנקבעו בתקנות שעת החירום השניות, וכן להאריך את תקופת תוקפו של החוק נוכח ההערכות המקצועיות כאמור לעיל.

לנוכח הערכת גורמי המקצוע כי במרחב הקיברנטי הלחימה תוסיף להתנהל בעצימות גבוהה אף במנותק ממצב הלחימה במסגרת חרבות ברזל, באופן המצדיק את הקניית הכלים והסמכויות האמורות, מוצע לקבוע כי הפעלת הכלים והסמכויות מכוח החוק לא יהיו תלויים במצב הלחימה כאמור. וזאת לתקופה זמנית במסגרת הוראת שעה.

החוק המוצע בא להחליף את ההסדר שנקבע בתקנות שעת החירום ועל כן מוצע לבטלן (ראו סעיף 12 להצעת החוק).

סעיף 1 כאמור, מגמת העלייה בהיקפן ובמורכבותן של תקיפות הסייבר במרחב הסייבר הישראלי, ובייחוד כלפי מגזר השירותים הדיגיטליים ושירותי האחסון, התחדדה עם פרוץ חרבות ברזל. בשל כך, נקבע ההסדר שבחוק כהסדר שחל במהלך תקופת חרבות ברזל, כך שההגדרה של תקיפת סייבר כתקיפת סייבר חמורה בחוק, מותנית כיום, בין השאר, בהתרחשותה במהלך תקופת הפעולות הצבאיות המשמעותיות (חרבות ברזל). לצד זאת, כאמור, בהתאם להערכות המקצועיות של הגופים לגבי חומרת איומי הסייבר העדכניים והסיכונים המשמעותיים הנשקפים מהם, ובשל מאפייניו הייחודיים של מרחב הסייבר הישראלי, הצורך בסמכויות ובכלים לצורך התמודדות ראויה עם תקיפות חמורות במרחב הסייבר הישראלי עומד בעינו, וזאת אם תיפסק הלחימה במסגרת חרבות ברזל. לפיכך, הסמכויות והכלים החיוניים, אשר נקבעו במסגרת החוק ותקנות שעת החירום הנחוצים להתמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון, נדרשים לשם שמירה על ביטחון המדינה, ביטחון הציבור או למניעת פגיעה באופן חמור ברציפות אספקתם של שירותים חיוניים לציבור, וזאת אף במנותק מן הלחימה במסגרת חרבות ברזל ומהמערכה הקינטית מול איראן. על כן, מוצע לקבוע שההסדר הקבוע בחוק יחול בלא תלות בהימשכות הפעולות הצבאיות המשמעותיות ובמצב הלחימה במסגרת חרבות ברזל. בהתאם לכך, מוצע לשנות את שמו של החוק כך שהמילים "חרבות ברזל" יימחקו ממנו.

סעיף 2 מוצע לתקן את סעיף 1 לחוק, סעיף ההגדרות, ולהוסיף הגדרות נוספות שנקבעו בתקנות שעת החירום השניות כדי לעגן הוראות מהותיות שנקבעו בתקנות אלה, וכן למחוק הגדרות המתייחסות ללחימה במסגרת חרבות ברזל כחלק מניתוק החוק ממצב הלחימה.

בין השאר, מוצע לקבוע בסעיף 3(ב) לחוק את החובה המוטלת על ספק אשר מותקף בתקיפת סייבר חמורה לידע ארגון מקושר אשר עלול להיפגע ממנה ישירות ובאופן ממשי. לעניין זה, מוצע להגדיר "ארגון מקושר" כארגון שקיים חיבור, פיזי או לוגי, קבוע או עיתי, בין מחשביו לבין מחשבי הספק, או שמתבצעת העברת חומר מחשב, קבועה או עיתית, בין מחשבי הספק למחשביו. כלומר, ארגון מקושר הוא ארגון שקיימת חיבוריות בין מחשביו למחשבי הספק, שבגינה קיימת סכנה להתפשטות התקיפה מהספק לארגון.

כמו כן, מוצע לקבוע כי "המרכז הלאומי", שבאמצעותו ידווח ספק על תקיפת סייבר משמעותית בהתאם לסעיף 2א לחוק, הוא המרכז הלאומי לסיוע בהתמודדות עם איומי סייבר (CERT) שפועל במערך הסייבר הלאומי, וכן לתקן את ההגדרות "מנהל מוסמך" ו"עובד מוסמך" לעניין המלמ"ב, כך שבמקום "ראש היחידה הטכנולוגית במלמ"ב" יבוא "ראש יחידת הסייבר במלמ"ב", ובהתאם, בהגדרה "עובד מוסמך", במקום "היחידה הטכנולוגית" יבוא "יחידת הסייבר".

נוסף על כך, מוצע למחוק את ההגדרה "הפעולות הצבאיות המשמעותיות" וזאת במסגרת ניתוק הזיקה של החוק והפעלת הסמכויות מכוחו לפעולות הצבאיות המשמעותיות, כאמור לעיל.

(2) בהגדרה "מנהל מוסמך", במקום פסקה (3) יבוא:

"(3) לעניין ספק של הגופים המנויים בפרטים 2 ו־3 לתוספת הראשונה לחוק להסדרת הביטחון – ראש יחידת הסייבר במלמ"ב;";

(3) אחרי ההגדרה "מערך הסייבר" יבוא:

""המרכז הלאומי" – המרכז הלאומי לסיוע בהתמודדות עם איומי סייבר (CERT), שמפעיל מערך הסייבר;";

(4) בהגדרה "עובד מוסמך", בפסקה (3), במקום "היחידה הטכנולוגית" יבוא "יחידת הסייבר";

(5) ההגדרה "הפעולות הצבאיות המשמעותיות" – תימחק.

תיקון סעיף 2

3. בסעיף 2(א) לחוק העיקרי –

(1) ברישה, במקום "בביטחון הציבור או בקיום האספקה והשירותים החיוניים" יבוא "או בביטחון הציבור או לפגוע באופן חמור ברציפות אספקתם של שירותים חיוניים לציבור";

(2) פסקה (1) – תימחק;

(3) אחרי סעיף קטן (א) יבוא:

"(א1) היה למנהל מוסמך יסוד סביר להניח כי תקיפת סייבר שמתרחשת או שיש חשש ממשי כי היא עומדת להתרחש, היא תקיפת סייבר חמורה נגד ספק או תקיפה כאמור הנעשית באמצעות ספק, רשאי הוא, בעצמו או באמצעות עובד מוסמך, לדרוש מהספק להציג לו כל ידיעה או מסמך לרבות פלט, כדי להבטיח את ביצועו של סעיף זה או להקל את ביצועו; הוראות סעיף קטן זה לא יחולו לעניין ספק שהגיש תצהיר כאמור בסעיף 3(א)(3).";

(4) בסעיף קטן (ב), במקום "בפסקאות (1) עד (3)" יבוא "בפסקאות (2) ו־(3)".

דברי הסבר

סעיף 3 כמפורט לעיל, ובשל מאפייניו הייחודיים של מרחב הסייבר, מוצע לקבוע שההסדר יחול בלא תלות בהימשכות הפעולות הצבאיות המשמעותיות. בהתאם, מוצע לתקן את העילה שלפיה יקבע מנהל מוסמך שיש חשש ממשי לתקיפת סייבר חמורה. כך, לפי הנוסח המוצע, המנהל המוסמך יידרש לבחון אם יש חשש ממשי שיש בתקיפת הסייבר כדי לפגוע בביטחון המדינה או בביטחון הציבור או לפגוע באופן חמור ברציפות אספקתם של שירותים חיוניים לציבור.

במקביל, מוצע למחוק מרשימת התבחינים להגדרתה של תקיפת סייבר כתקיפת סייבר חמורה על ידי המנהל המוסמך בהתאם לסעיף 2 לחוק, את התבחין הקבוע בסעיף 2(א)(1) לחוק, שלפיו על התקיפה להתרחש במהלך תקופת הפעולות הצבאיות המשמעותיות.

נוסף על כך, מוצע להוסיף לסעיף 2 לחוק את סעיף קטן (א1) ולקבוע בו שכאשר למנהל מוסמך יש יסוד סביר להניח שתקיפת סייבר שמתרחשת, או שקיים חשש ממשי כי עומדת להתרחש, נגד ספק או באמצעות הספק, היא תקיפת סייבר חמורה, הוא רשאי, בעצמו או באמצעות עובד מוסמך, לדרוש מהספק להציג לו כל ידיעה או מסמך, לרבות פלט מחשב, וזאת כדי להבטיח את ביצועו של סעיף 2 או להקל את ביצועו. זאת, לצורך בחינת התקיימותם של התנאים לקביעה שתקיפת סייבר שמתרחשת או שיש חשש ממשי שעומדת להתרחש היא תקיפה חמורה לפי סעיף 2(א) לחוק.

כמו כן, בהתאם לסעיף 4 לחוק, כתיקונו בהצעת חוק זו, הדרישה להעברת ידיעות או מסמכים תתועד בכתב ויימסר לספק נוסח כתוב של הדרישה שאינו מכיל מידע מסווג, בהקדם האפשרי לאחר הדרישה. יובהר שפניית מנהל מוסמך לספק, לצורך דרישת ידיעות ומסמכים, תבוצע באופן מצומצם והדרגתי ככל הניתן, בשים לב לנתונים הקיימים בידי המנהל המוסמך ולמידע המינימלי הנדרש לבחינת חומרת תקיפת הסייבר המסוימת. כך לדוגמה, ככל שלצורך קבלת החלטה אם התקיפה הנבחנת היא תקיפת סייבר חמורה, נדרש למנהל המוסמך מידע בנוגע לקישוריות הספק לארגונים אחרים לשם הערכת הסיכון הנגזר מן התקיפה, תתמקד דרישת המידע הראשונית במידע הנוגע לכך. עוד לשם המחשה, במקרה שבו קיים ספק באשר למאפיינים הטכנולוגיים של התקיפה לשם הבנת חומרתה, תתמקד הפנייה הראשונית של המנהל

הוספת סעיף 2א

4. אחרי סעיף 2 לחוק העיקרי יבוא:

"חובת דיווח

2א. (א) נודע לספק על כך שמתרחשת נגדו, בפועל, תקיפת סייבר שמתקיים לגביה אחד מאלה, ידווח על כך למנהל המוסמך באמצעות המרכז הלאומי, בהתאם להוראות סעיף קטן (ב):

(1) יש חשש ממשי שהיא אינה מוגבלת לספק הנתקף;

(2) היא עלולה לפגוע באופן משמעותי בזמינות, ברציפות או במהימנות השירות של הספק, בהתחשב, בין השאר, באלה:

(א) כמות או סוג המשתמשים בשירות, שעלולים להיות מושפעים מהתקיפה;

(ב) סוג הפגיעה והיקפה;

(ג) משך הפגיעה.

דברי הסבר

המוסמך, ככל האפשר, בדרישה ממוקדת לקבלת המאפיינים הטכנולוגיים הנדרשים לצורך הבחינה האמורה. עוד מוצע לקבוע כי ספק אשר הגיש תצהיר בדבר עמידה בתקנים כמפורט בתוספת, לעניין כלל השירותים כאמור שהוא מספק, או לעניין השירותים כאמור, שנגדם בוצעה התקיפה, לא יידרש למסור ידיעות או מסמכים לבחינת התקיימותה של תקיפת סייבר חמורה, בהתאם לסעיף 2(א1) לחוק כנוסחו המוצע.

סעיף 4 מוצע להוסיף לחוק את סעיף 2א, ולקבוע בו, שספק ידווח באופן מיידי למנהל מוסמך באמצעות המרכז הלאומי אם נודע לו על תקיפת סייבר המתרחשת נגדו בפועל, אשר יש חשש ממשי שהיא אינה מוגבלת לספק הנתקף, או אם התקיפה עלולה לפגוע באופן משמעותי בזמינות, ברציפות או במהימנות שירותי הספק. לצורך בחינת התקיימותו של התנאי השני, הספק ישקול שיקולים שונים, ובהם: כמות או סוג המשתמשים העלולים להיות מושפעים מהתקיפה, סוג והיקף הפגיעה וכן את משך הפגיעה.

עוד מוצע לקבוע כי הדיווח שאותו יעביר הספק למנהל המוסמך, לפי סעיף זה, ייעשה באחת משתי דרכים שלהלן, לפי בחירתו, ואולם לאחר שבחר הספק בדרך מסוימת, הוא לא יוכל לשנות את בחירתו:

החלופה הראשונה היא דיווח מיידי, בלא דיחוי ובהקדם האפשרי, הכולל את הפרטים שלהלן, ככל שהם ידועים לספק, וכל מידע אחר שיש בו כדי לסייע להערכת חומרתה של תקיפת הסייבר והשלכותיה:

1. פרטי הספק והשירותים שהוא מספק, ובכלל זה פרטי קשר שלו;
2. מועד תחילת תקיפת הסייבר ומועד גילויה;
3. מידע לגבי מאפייני התקיפה והשפעתה על הספק;
4. מידע הנוגע לאפשרות השפעת התקיפה על ארגונים מקושרים, כלומר ארגון שקיים קישור לוגי או פיזי בינו לבין הספק, קבוע או עיתי, או שמתבצעת העברת חומר מחשב קבועה או עיתית, ממחשביו למחשבי מקבל שירותיו.

החלופה השנייה היא חלופת דיווח אשר מטרתה המרכזית להקל על ספקים שחלה לגביהם חובת דיווח בהתאם לדירקטיבת האיחוד האירופי (Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for High Common Level of Cybersecurity Across the Union) (להלן – דירקטיבת NIS2), ולאפשר דיווח דומה. בהתאמה לקבוע בדירקטיבת NIS2, מוצע לקבוע בחלופת דיווח זו שספק יגיש בלא דיחוי ובתוך 24 שעות מהמועד שבו נודע לו על התקיפה, דיווח ראשוני על תקיפת הסייבר, הכולל מידע שיש בו כדי לסייע בהערכת חומרת התקיפה והשלכותיה, אם הוא ידוע לו, וכן פרטי הספק והשירותים שהוא מספק, ובכלל זה פרטי קשר שלו.

עוד מוצע לקבוע במסגרת חלופה זו, בהתאם לקבוע בדירקטיבת NIS2, שספק יגיש בלא דיחוי ולא יאוחר מחלוף 72 שעות מהמועד שבו נודע לו על תקיפת הסייבר, דיווח שיכלול עדכון לגבי המידע שנמסר בדיווח הראשוני; הערכה ראשונית בדבר חומרת התקיפה והשלכותיה; ומידע הנוגע למאפייני תקיפת הסייבר ולמזהי התקיפה, והכול אם המידע האמור ידוע לו.

נוסף על כך, בדומה לקבוע בדירקטיבת NIS2, מוצע לקבוע, במסגרת חלופה זו, שמנהל מוסמך יהיה רשאי, בעצמו או באמצעות עובד מוסמך, לדרוש דיווח ביניים הכולל עדכון לגבי המידע שנמסר בדיווח הראשוני או בדיווח שנמסר לאחר 72 שעות מהמועד שבו נודע לספק על תקיפת הסייבר כאמור.

כמו כן, בדומה לקבוע בדירקטיבת NIS2, מוצע לקבוע בחלופה זו, שהספק יגיש דיווח מסכם, וזאת לא יאוחר מ־30 ימים מהמועד שבו הגיש את הדו"ח לפי פסקת משנה (ב) המוצעת (הדו"ח שמוגש כעבור 72 שעות מהמועד שנודע

(ב) לשם מילוי חובתו כאמור בסעיף קטן (א), יפעל ספק באחת הדרכים שבפסקאות (1) או (2) להלן, בציון הדרך שבה בחר לפעול:

(1) יגיש, באופן מיידי, דיווח הכולל את הפרטים שלהלן, אם הם ידועים לו, וכל מידע אחר שיש בו כדי לסייע להערכת חומרתה של תקיפת הסייבר והשלכותיה:

(א) פרטי הספק והשירותים שהוא מספק, ובכלל זה פרטי קשר שלו;

(ב) מועד תחילת תקיפת הסייבר ומועד גילויה;

(ג) מידע לגבי מאפייני תקיפת הסייבר והשפעתה על הספק;

(ד) מידע הנוגע לאפשרות שהתקיפה תשפיע באופן ממשי על ארגון מקושר;

(2) יגיש, בהתאם למפורט בפסקאות משנה (א) עד (ה) שלהלן, את הדיווחים כמפורט בהן:

(א) יגיש, בלא דיחוי ולא יאוחר מחלוף 24 שעות מהמועד שבו נודע לספק על תקיפת הסייבר, דיווח ראשוני על תקיפת הסייבר הכולל מידע שיש בו כדי לסייע בהערכת חומרת התקיפה והשלכותיה, אם הוא ידוע לו, וכן את פרטי הספק והשירותים שהוא מספק, ובכלל זה פרטי קשר שלו;

(ב) יגיש, בלא דיחוי ולא יאוחר מחלוף 72 שעות מהמועד שבו נודע לספק על תקיפת הסייבר, דיווח הכולל עדכון לגבי המידע שנמסר בדיווח הראשוני כאמור בפסקת משנה (א), הערכה ראשונית בדבר חומרת התקיפה והשלכותיה, ומידע הנוגע למאפייני תקיפת הסייבר ולמזהי התקיפה, והכול אם המידע האמור ידוע לו;

(ג) יגיש, לפי דרישה מאת המנהל המוסמך, בעצמו או באמצעות עובד מוסמך ובמועד שיקבע המנהל המוסמך, דיווח ביניים הכולל עדכון לגבי המידע שנמסר לפי פסקאות משנה (א) או (ב);

דברי הסבר

לספק על תקיפת הסייבר), הכולל תיאור מפורט על אודות תקיפת הסייבר, לרבות חומרתה והשלכותיה; סוג התקיפה והגורמים שהיוו מקור להתרחשות התקיפה, ככל שהם ידועים לספק; אופן הטיפול בתקיפה, לרבות פירוט בדבר אמצעים שננקטו או שעדיין ננקטים לצורך כך, למעט סוד מסחרי הנוגע ישירות לאופן הטיפול ולאמצעים כאמור.

עוד מוצע לקבוע במסגרת חלופה זו, שאם לא הסתיים הטיפול בתקיפת הסייבר בתוך 30 ימים, הספק יגיש באותו מועד, דיווח על אודות התקדמות הטיפול בתקיפת הסייבר, הכולל את הפרטים הידועים לספק מתוך הפרטים שעליו לדווח במסגרת הדיווח המסכם, ויגיש גם דיווח מסכם, לא יאוחר מ־30 ימים לאחר סיום הטיפול בתקיפה.

עוד מוצע לקבוע שדיווח לפי סעיף זה יכול שיוגש באופן מקוון באתר האינטרנט של מערך הסייבר הלאומי, בהודעה טלפונית למרכז הלאומי, או בדרך אחרת שיורה ראש מערך הסייבר הלאומי ותפורסם באתר האינטרנט האמור.

כמו כן, מוצע לקבוע כי ספק של הגופים המנויים בסעיף 2 ובסעיף 3 לתוספת הראשונה לחוק להסדרת

(ד) יגיש, לא יאוחר מחלוף 30 ימים מהמועד שבו הגיש את הדיווח לפי פסקת משנה (ב), דיווח הכולל את הפרטים שלהלן (להלן – דיווח מסכם):

(1) תיאור מפורט על אודות תקיפת הסייבר, לרבות חומרתה והשלכותיה;

(2) סוג התקיפה והגורמים שהיוו מקור להתרחשותה, לפי מיטב ידיעתו של הספק;

(3) אופן הטיפול בתקיפה, לרבות פירוט בדבר אמצעים שננקטו או שעדיין ננקטים לצורך כך, למעט סוד מסחרי הנוגע ישירות לאופן הטיפול בתקיפה ולאמצעים כאמור;

(ה) על אף האמור בפסקת משנה (ד), אם לא הסתיים הטיפול בתקיפת הסייבר במועד הדיווח כאמור באותה פסקת משנה, יגיש הספק, באותו מועד, דיווח על התקדמות הטיפול בתקיפת הסייבר, הכולל את הפרטים לפי אותה פסקת משנה, אם הם ידועים לו; הסתיים הטיפול בתקיפה, יגיש הספק, לא יאוחר מ־30 ימים לאחר סיום הטיפול בתקיפה, דיווח מסכם כאמור באותה פסקת משנה.

(ג) דיווח לפי סעיף זה יכול שיוגש באופן מקוון באתר האינטרנט של מערך הסייבר הלאומי, בהודעה טלפונית למרכז הלאומי או בדרך אחרת שהורה עליה ראש מערך הסייבר הלאומי ופורסמה באתר האינטרנט כאמור.

(ד) על אף האמור בסעיף קטן (ג), ספק של גוף מהגופים המנויים בפרטים 2 ו־3 לתוספת הראשונה לחוק להסדרת הביטחון, יגיש את הדיווח לפי סעיף זה למלמ"ב, באופן שיורה לו ראש המלמ"ב."

תיקון סעיף 3

5. בסעיף 3 לחוק העיקרי –

(1) האמור בו יסומן "(א)" ובו –

(א) ברישה, אחרי "נגד ספק" יבוא "או באמצעותו";

(ב) בפסקה (3), במקום "בהתאם לתקן המנוי בתוספת הראשונה או לפיה" יבוא "בהתאם לאמור בטור א' לתוספת", ואחרי "שנגדם בוצעה התקיפה" יבוא "ואם מנוי בטור ב' לצידו מסמך – בצירוף המסמך";

(2) אחרי סעיף קטן (א) יבוא:

דברי הסבר

הביטחון בגופים ציבוריים, התשנ"ח–1998, כלומר – משרד הביטחון, מפעלי מערכת הביטחון ומפעלים המייצרים מוצרים בעבור מערכת הביטחון, שהוגדרו בצו על ידי שר הביטחון, יגיש את הדיווח על תקיפת הסייבר נגדו למלמ"ב, באופן שיורה לו ראש המלמ"ב.

סעיף 5 מוצע להבהיר, ברישה של סעיף 3(א) לחוק, שהוראות החוק ביחס לתקיפה חמורה, חלות הן כשתקיפת סייבר מתרחשת או עומדת להתרחש נגד ספק והן כשתקיפה כאמור מתקיימת באמצעותו.

"(ב) (1) מסר העובד המוסמך לספק הודעה כאמור בסעיף קטן (א), ימסור הספק, בלא דיחוי, עדכון בדבר התקיפה החמורה לכל ארגון מקושר אשר עלול להיפגע ממנה ישירות ובאופן ממשי, וידווח על כך בכתב לעובד המוסמך, והכול אלא אם כן הורה העובד המוסמך אחרת; הוראות סעיף קטן זה לא יחולו לעניין ספק שהגיש תצהיר כאמור בסעיף קטן (א)(3).

(2) המנהל המוסמך רשאי, לפי בקשה בכתב מאת הספק, אם שוכנע כי קיימות נסיבות חריגות המצדיקות זאת, לפטור את הספק מחובת היידוע כאמור בפסקה (1) או לדחות את מועד היידוע."

תיקון סעיף 4

6. בסעיף 4 לחוק העיקרי, במקום "שנתן לספק לפי סעיף 3" יבוא "שניתנו לספק לפי סעיפים 2(א1), 2א(ב)(2)(ג) או 3".

דברי הסבר

כמו כן, בשים לב לחיבוריות הגבוהה במגזר השירותים הדיגיטליים ושירותי האחסון ולנוכח הצורך למנוע התפשטות תקיפות סייבר חמורות, מוצע לתקן את סעיף 3 לחוק כך שיתווסף לו סעיף קטן (ב), ולקבוע בו שלאחר שקיבל הספק את הודעת העובד המוסמך על כך שתקיפת סייבר שמתרחשת או עומדת להתרחש נגדו היא תקיפת סייבר חמורה, הוא יידע, בלא דיחוי, כל ארגון מקושר שעלול להיפגע ישירות ובאופן ממשי מהתקיפה האמורה, וידווח על כך לעובד המוסמך. עוד מוצע לקבוע, כי חובת היידוע לפי סעיף קטן מוצע זה, לא תחול אם הורה על כך העובד המוסמך, או שהמנהל המוסמך מצא כי מתקיימות נסיבות המצדיקות זאת, לבקשת הספק.

בהתאם לסעיף 3(א)(3) לחוק, כיום, באפשרות הספק למסור תצהיר, כמפורט בתוספת לחוק, בדבר יישום הנחיות אבטחה בהתאם לתקן הבין־לאומי NIST 800–53 Security and Privacy Controls for Information Systems and Organizations.

מוצע לקבוע בסעיף 3(א)(3) לחוק כתיקונו המוצע, שספק אשר יצהיר על אספקת שירותי אחסון או שירותים דיגיטליים ללקוחותיו של הספק או בדבר אספקת שירותי תחזוקה, ניהול או בקרה של שירותים כאמור ללקוחותיו של הספק, תוך יישום הנחיות אבטחה בהתאם לתקנים המנויים בתוספת, ובכלל האמור שילוב בין התקנים, כמפורט בתוספת, וזאת לעניין כלל השירותים כאמור שהוא מספק, או לעניין השירותים כאמור שנגדם בוצעה התקיפה, יחול לגביו הסדר ייחודי, ובכללו הוא לא יידרש למסור ידיעות או מסמכים לבחינת התקיימותה של תקיפת סייבר חמורה בהתאם לסעיף 2(א1) לחוק כנוסחו בהצעת חוק זו, לא יינתנו לו הוראות לפי סעיף 3(א)(4) לחוק וכן הוא יהיה פטור מן החובה לעדכן ארגון מקושר על תקיפות סייבר חמורות בהתאם לסעיף 3(ב) לחוק כנוסחו המוצע.

יצוין כי מדובר בתקנים בין־לאומיים מקצועיים שיש בהם כדי לתת מענה לתקיפות מורכבות. עמידה בדרישות המפורטות בתקנים אלה, אשר מוכרים ונגישים במגזר השירותים הדיגיטליים ושירותי האחסון, מעידה על יכולת התמודדות טובה עם איומי סייבר, המביאה לצמצום משמעותי של הסיכון הנשקף מתקיפת סייבר אצל ספק.

רשימת התקנים והשילובים ביניהם, נבחרו מאחר שלגופים העומדים בהם יש נהלים, מדיניות ארגונית ותהליכים ארגוניים שמבטיחים טיפול הולם בתקיפות חמורות. ספק המוסמך לפי אחד או יותר מתקני הליבה המנויים בתצהיר מפגין רמה יחסית גבוהה של מוכנות ניהולית ותהליכית בהתמודדות עם איומי סייבר. הסמכה כאמור מעידה על כך שהארגון מיישם גישה שיטתית לזיהוי ולניהול סיכונים, מחזיק במדיניות סדורה, מבצע מיפוי תהליכים ונכסים, ומפעיל בקרות להגנה, זיהוי, תגובה ושיקום. נוסף על כך, קיימת התמקדות בהגברת המודעות הארגונית ובהטמעת תהליכים מבוססי Best Practices, תוך שילוב אחריות הנהלה גבוהה. העמידה בתקנים אלה מבטאת יישום של עקרונות חוסן דיגיטלי והיערכות מקצועית להתמודדות עם תרחישים מורכבים. תקנים אלה מהווים מסגרת יציבה ואמינה ליצירת מערך אבטחת מידע והגנת סייבר מודרנית, והם תומכים ביישום רציף של שיפור ותחזוקה של מערך הסייבר הארגוני – הן ברמה הניהולית והן ברמה האופרטיבית.

לצד אלה, התקנים המשלימים המנויים בתוספת משמשים חיזוק נקודתי במרחבי סיכון ייחודיים, כגון פיתוח מאובטח, אבטחת ענן, פרטיות, ICS, שרשרת אספקה ותגובה לאירועים. שילוב בין תקן ליבה ותקן משלים מספק כיסוי רוחבי סביר ועומק הגנתי המהווים יחדיו מענה טוב לתקיפות סייבר חמורות.

סעיף 6 סעיף 4 לחוק קובע שעובד מוסמך יתעד בכתב את ההוראות שניתנו לספק לפי סעיף 3 לחוק וימסור לאותו ספק, בהקדם האפשרי לאחר מתן ההוראה, נוסח כתוב של ההוראות, שאינו מכיל מידע מסווג. לנוכח התיקונים בהצעת חוק זו, מוצע להוסיף חובת תיעוד דומה

תיקון סעיף 6

7. בסעיף 6(ב) לחוק העיקרי, אחרי "בתקיפת הסייבר החמורה" יבוא "ולעניין תקיפת סייבר שנקבע, לפי הוראות סעיף 2, שהיא אינה תקיפת סייבר חמורה – בסמוך לאחר קבלת החלטה על כך שהתקיפה אינה מהווה תקיפת סייבר חמורה".

תיקון סעיף 8

8. בסעיף 8(א) לחוק העיקרי –

(1) בפסקאות (1) ו־(1א), במקום "סעיף 3(4)" יבוא "סעיף 3(א)(4)";

(2) בפסקה (2), במקום "סעיף 3" יבוא "סעיף 3(א)";

(3) אחרי פסקה (4) יבוא:

"(5) מספר המקרים שבהם דיווח ספק, לפי הוראות סעיף 2א, על כך שמתרחשת נגדו תקיפת סייבר כאמור באותו סעיף;

(6) מספר המקרים שבהם הורה עובד מוסמך לספק שלא למסור לארגון מקושר עדכון בדבר תקיפת סייבר חמורה, לפי הוראות סעיף 3(ב)(1)."

תיקון סעיף 10

9. בסעיף 10 לחוק העיקרי, בפרט 65 בתוספת הראשונה לחוק בתי משפט לעניינים מינהליים, התש"ס–2000[2], המובא בו, במקום "(הוראת שעה – חרבות ברזל)" יבוא "(הוראת שעה)".

תיקון סעיף 12

10. בסעיף 12 לחוק העיקרי, במקום "כ"ו בחשוון התשפ"ו (17 בנובמבר 2025)" יבוא " ז' בניסן התשפ"ו (25 במרץ 2026)".

החלפת התוספת

11. במקום התוספת לחוק העיקרי יבוא:

דברי הסבר

על ידי העובד המוסמך גם ביחס לדרישת ידיעות ומסמכים של המנהל המוסמך לפי סעיף 2(א1) לחוק כנוסחו המוצע וביחס לדרישה של מנהל מוסמך לקבלת דיווח ביניים לפי סעיף 2א(ב)(2)(ג) המוצע.

סעיף 7 במסגרת ההסדר הקיים, סעיף 6(ב) לחוק קובע שמידע שהתקבל מספק לפי הוראות החוק, יימחק בסמוך לאחר סיום הטיפול בתקיפת הסייבר החמורה, אלא אם כן קבע מנהל מוסמך שהמידע כאמור חיוני לזיהוי מאפייני תקיפת הסייבר. מוצע לתקן את סעיף 6(ב) האמור תוך הוספת הקביעה כי לעניין תקיפת סייבר שנקבע לגביה, לפי הוראות סעיף 2 לחוק, שהיא אינה תקיפת סייבר חמורה, יימחק המידע בסמוך לאחר קבלת החלטה על כך שהתקיפה אינה מהווה תקיפת סייבר חמורה, אלא אם כן קבע מנהל מוסמך שהמידע חיוני לזיהוי מאפייני תקיפת הסייבר. מידע שנקבע לגביו כאמור, יישמר בהיקף המזערי הנדרש.

סעיף 8 לשם קיום פיקוח ובקרה שוטפים על פעולותיהם של הגורמים המוסמכים לפי הוראות חוק זה, מוצע לקבוע כי תורחב חובת הדיווח ליועץ המשפטי לממשלה ולוועדת החוץ והביטחון של הכנסת, הקבועה בסעיף 8 לחוק, כך שתתווסף חובת דיווח לעניין מספר המקרים שבהם דיווח ספק, לפי הוראות סעיף 2א לחוק, כנוסחו בהצעת חוק זו, על כך שמתרחשת נגדו תקיפת סייבר לפי הסעיף האמור, וכן לעניין מספר המקרים שבהם הורה עובד מוסמך לספק שלא למסור לארגון מקושר עדכון בדבר תקיפת סייבר חמורה, לפי הוראות סעיף 3(ב)(1) לחוק כנוסחו בהצעת חוק זו.

סעיף 9 מוצע לערוך התאמה בפרט 65 לתוספת הראשונה לחוק בתי משפט לעניינים מינהליים, התש"ס–2000, המובא בסעיף 10 לחוק, בעקבות שינוי שם החוק כמוצע בסעיף 1 להצעת החוק.

סעיף 10 לנוכח האיומים והערכות של גורמי המקצוע בגופים, כמתואר לעיל, וכן הצורך במתן פרק זמן שיאפשר לבחון את אופן יישומם של ההסדרים החדשים המוצעים, מוצע להאריך את תוקפו של החוק, כהוראת שעה, עד יום ז' בניסן התשפ"ו (25 במרץ 2026).

סעיף 11 כאמור, במסגרת הצעת החוק מוצע לקבוע כי ספק שהגיש תצהיר בדבר אספקת שירותי אחסון או שירותים דיגיטליים ללקוחותיו של הספק או בדבר אספקת שירותי תחזוקה, ניהול או בקרה של שירותים כאמור ללקוחותיו של הספק, תוך יישום הנחיות אבטחה בהתאם לתקנים המנויים בתוספת, לפי העניין, לעניין כלל השירותים כאמור שהוא מספק או לעניין השירותים כאמור שנגדם בוצעה התקיפה, יהיה פטור מן הדרישה למסור ידיעות או מסמכים לבחינת התקיימותה של תקיפת סייבר חמורה בהתאם לסעיף 2(א1) לחוק כנוסחו המוצע בהצעת חוק זו; לא יינתנו לו הוראות לפי סעיף 3(א)(4) לחוק; וכן

[2] ס"ח התש"ס, עמ' 192.

"תוספת

(סעיף 3(א)(3))

	טור א' התקן	טור ב' המסמך
1.	הספק מיישם את הדרישות לצורך עמידה בתקן NIST 800–53 Security and Privacy Controls for Information Systems and Organizations (high);	
2.	הספק מיישם את הדרישות לצורך עמידה בשניים מתקני הליבה שלהלן:	
	(1) ISO/IEC 27001 או ת"י 27001	תעודת הסמכה בתוקף
	(2) SOC 2 Type 2	תעודת הסמכה או דוח Attestation בתוקף
	(3) CMMC Level 3	תעודת הסמכה או דוח הערכה (Assessment) על ידי DCMA DIBCAC (Defense Contract Management Agency – Defense Industrial Base Cybersecurity Assessment Center)
	(4) NIST 800–53 Security and Privacy Controls for Information Systems and Organizations (Moderate)	מסמך Authorization To Operate (ATO) קבוע ובתוקף, החתום על ידי Authorizing Official (AO) מוסמך מטעם סוכנות פדרלית, משרד ממשלתי או גוף ציבורי אחר בארצות הברית, ומצורף בלי תנאים מגבילים (ATO with Conditions) ובלי פריטי Plan of Action and Milestones (POA&M), שמועד הטיפול בהם חלף במועד הגשת התצהיר, וזאת בהתאם לרמת Moderate.
3.	הספק מקיים את שני אלה:	
	(1) הספק מיישם את הדרישות לצורך עמידה בתקן אחד מתקני הליבה שלהלן ומצורף אישור כמפורט לצידו, וכמו כן הספק מקיים את הבקרות הנדרשות בהתאם לתקן נוסף מתקני הליבה שלהלן:	
	(א) ISO/IEC 27001 או ת"י 27001	תעודת הסמכה בתוקף

טור א׳ התקן		טור ב׳ המסמך
(ב)	SOC 2 Type 2	תעודת הסמכה או דוח אימות תאימות (Attestation) בתוקף
(ג)	CMMC Level 3	תעודת הסמכה או דוח הערכה (Assessment) על ידי DCMA DIBCAC (Defense Contract Management Agency – Defense Industrial Base Cybersecurity Assessment Center)
(ד)	NIST 800–53 Security and Privacy Controls for Information Systems and Organizations (Moderate)	מסמך Authorization To Operate (ATO) קבוע ובתוקף, החתום על ידי Authorizing Official (AO) מוסמך מטעם סוכנות פדרלית, משרד ממשלתי או גוף ציבורי אחר בארצות הברית, ומצורף בלי תנאים מגבילים (ATO with Conditions) ובלי פריטי Plan of Action and Milestones (POA&M), שמועד הטיפול בהם חלף במועד הגשת התצהיר, וזאת בהתאם לרמת Moderate
(2)	הספק מיישם את הדרישות לצורך עמידה בתקן אחד מהתקנים המשלימים שלהלן:	
(א)	תקן ISO/IEC 27017	
(ב)	תקן ISO/IEC 27018	
(ג)	תקן ISO/IEC 27034	
(ד)	תקן ISO/IEC 27035	
(ה)	תקן ISO/IEC 27701	תעודת הסמכה
(ו)	תקן PCI DSS	
(ז)	תקן IEC 62443	
(ח)	תקן ISO 22301	
(ט)	תקן SOC 2 Type 1	
(י)	תקן ״רב מגן״ ברמה 2	אישור בכתב מאת משרד הביטחון
(יא)	תקן CIS – Critical Security Control (IG3)	דוח אימות תאימות מאת CIS Securesuite Members

טור א׳ התקן	טור ב׳ המסמך
4. הספק מקיים את כל אלה:	
(1) הספק מיישם את הדרישות לצורך עמידה בתקן אחד מהתקנים שלהלן:	
(א) CMMC Level 3	תעודת הסמכה או דוח הערכה (Assessment) על ידי DCMA DIBCAC (Defense Contract Management Agency – Defense Industrial Base Cybersecurity Assessment Center)
(ב) NIST 800–53 Security and Privacy Controls for Information Systems and Organizations (Moderate)	מסמך ATO (Authorization To Operate) קבוע ובתוקף, החתום על ידי Authorizing Official (AO) מוסמך מטעם סוכנות פדרלית, משרד ממשלתי או גוף ציבורי אחר בארצות הברית, ומצורף בלא תנאים מגבילים ATO (with Conditions) ובלי פריטי Plan of Action and Milestones (POA&M), שמועד הטיפול בהם חלף במועד הגשת התצהיר, וזאת בהתאם לרמת Moderate
(2) הספק מקיים את הבקרות הנדרשות בהתאם לתקן אחד מתקני הליבה שלהלן:	
(א) ISO/IEC 27001 או ת"י 27001	
(ב) SOC 2 Type 2	
(3) הספק מקיים את הבקרות הנדרשות בהתאם לתקן אחד מהתקנים המשלימים שלהלן:	
(א) תקן ISO/IEC 27017	
(ב) תקן ISO/IEC 27018	
(ג) תקן ISO/IEC 27034	
(ד) תקן ISO/IEC 27035	
(ה) תקן ISO/IEC 27701	
(ו) תקן NIST SP 800–161	
(ז) תקן NIST SP 800–218	
(ח) תקן PCI DSS	

טור א׳ התקן	טור ב׳ המסמך
(ט) תקן IEC 62443	
(י) תקן ISO 22301	
(יא) תקן SOC 2 Type 1	
(יב) תקן "רב מגן" ברמה 2	
(יג) תקן CIS Critical Security Control (IG3)	דוח אימות תאימות מאת CIS Securesuite Members".

ביטול תקנות שעת חירום (חרבות ברזל) (סמכויות נוספות לשם התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון)

12. תקנות שעת חירום (חרבות ברזל) (סמכויות נוספות לשם התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון), התשפ"ה–2025[3] (להלן – תקנות שעת החירום) – בטלות.

הוראת מעבר

13. הוראות שניתנו ופעולות שבוצעו לפי תקנות שעת החירום, לפני תחילתו של חוק זה, יראו אותן כאילו נעשו לפי החוק העיקרי כנוסחו בחוק זה, והוראותיו יחולו עליהן.

דברי הסבר

הוא יהיה פטור מהחובה לעדכן ארגון מקושר על תקיפות סייבר חמורות בהתאם לסעיף 3(ב) לחוק.

בהתאם, מוצע לתקן את התוספת ולהוסיף לרשימת התקנים המנויים בה גם את החלופה של עמידה בשילובי תקנים, לצד צירוף המסמכים הנדרשים כמפורט בתוספת. חלופה נוספת זו תחליף את פרט 2 הקיים היום בתוספת לחוק, כך שתימחק האפשרות לקבוע תקינה נוספת באמצעות תיקון התוספת.

נוסף על כך, מוצע להוסיף את המונח High לפרט 1 בתוספת לחוק, שעניינו ברמה הגבוהה של התקן המנוי בה NIST 800–53 Security and Privacy Controls for Information Systems and Organizations. גוף המיישם קו בסיס אבטחה גבוה (High), נערך באופן מיטבי להתמודד עם תקיפות סייבר חמורות, שכן הוא מיישם סט מקיף של אמצעי הגנה, שנועדו להגן על סודיות, שלמות וזמינות המידע והמערכות, לנהל סיכוני אבטחה באופן פרואקטיבי ושיטתי, ולספק יכולת להגן על פעולות ונכסים קריטיים וחיוניים, באופן שמקים בסיס איתן לעמידות המערכות גם בפני האיומים החמורים ביותר.

סעיף 12 הצעת חוק זו באה להחליף את ההסדר שנקבע בתקנות שעת החירום השניות, ומוצע על כן לבטלן.

סעיף 13 לצד ביטול תקנות שעת החירום השניות, וכדי להבטיח את רציפות הדין בין אותן תקנות לבין תיקון החוק המוצע, מוצע לקבוע הוראת מעבר ולפיה יראו הוראות שניתנו ופעולות שבוצעו לפי תקנות שעת החירום האמורות, כאילו נעשו לפי החוק כנוסחו בחוק המוצע, והוראותיו יחולו עליהן.

[3] ק"ת התשפ"ה, עמ' 1974.