משרד החינוך

דוח ביקורת מיוחד - הגנת הסייבר על מערכות מידע במשרד החינוך ועל בחינות הבגרות וציוני הבגרות

דוח ביקורת מיוחד - הגנת הסייבר על מערכות מידע במשרד החינוך ועל בחינות הבגרות וציוני הבגרות

רקע

רוב המידע שמשרד החינוך אוסף, שומר ומנהל בעניין בחינות הבגרות וציוני הבגרות הוא מידע רגיש על תלמידים ועובדים, שכולל יותר מ-100,000 רשומות, ובהיותו כזה אבטחתו נדרשת להיות ברמה הגבוהה ביותר לפי תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (תקנות הגנת הפרטיות אבטחת מידע), ובכלל זה על משרד החינוך מוטלת החובה לשמור על המידע ולוודא שהוא משמש אך ורק למטרות שלשמן הוא נמסר או לצורכי מילוי חובותיו של המשרד על פי החוק. על המשרד לוודא כי המידע והנתונים לא ישונו או יימחקו, וכי הם ייחשפו רק לפני גורמים המורשים לקבל גישה אליהם, מתוקף תפקידם או מתוקף כך שהמידע נוגע להם, כגון התלמידים או הוריהם, או למוסדות השכלה גבוהה ולגורמים אחרים אשר תעודת הבגרות וציוני התלמידים נדרשים להם.

היבט נוסף המחייב נקיטה של אמצעים כדי למנוע פגיעה במאגרי מידע הוא תקיפות סייבר, ששכיחותן הולכת וגדלה והן גורמות לנזקים ניכרים ורחבי היקף. המניעים לכך שונים, ובהם כוונה לפגוע במערכות עצמן וכך לשבש את הפעילות התקינה והשוטפת של הארגון, החברה ואף המדינה, למטרת סחיטה, למטרת שינוי מידע כדי ליהנות מהטבות ומרווחים ואף במסגרת אתגר טכנולוגי לשמו.

נתוני מפתח

כ-1.39 מיליון
מחברות בחינה של תלמידים שנבחנו בבגרות הוערכו על ידי משרד החינוך בשנת הלימודים התשפ"א (ספטמבר 2020 - אוקטובר 2021)

כ-125,000
תלמידי כיתות י"ב נבחנו בבחינות הבגרות ב-1,299 בתי ספר בשנת הלימודים התשפ"א

כ-12,000
מחברות בחינה נמצאו חשודות כחריגות בשנת הלימודים התשפ"א

832
גרסאות שאלונים גובשו במשרד החינוך עבור 62 מקצועות לימוד בשנת הלימודים התשפ"א

כ-2,200
אירועי סייבר טופלו על ידי מערך הסייבר הלאומי בשנת 2021

33%
הגידול בשיעור אירועי הסייבר שבהם טיפל מערך הסייבר הלאומי בשנת 2021 לעומת השנה הקודמת

כ-467.6 מיליון ש"ח
תקציב אגף הבחינות במשרד החינוך בשנת 2021

כ-5% במקום 8%
שיעור תקציב הגנת הסייבר שהקצה משרד החינוך מתוך תקציב טכנולוגיות המידע בשנת 2020 (5%) לעומת החלטת הממשלה 2443 בעניין הגנת הסייבר המורה על 8%

פעולות הביקורת

בחודשים פברואר 2021 - מאי 2022 בדק משרד מבקר המדינה היבטים באבטחת המידע במשרד החינוך ואת אבטחת המידע של מערכות המידע המרכזיות שתומכות בניהול ובתפעול של ציוני בחינות הבגרות ובסביבות התקשוב שבהן הן פועלות. הבדיקה בוצעה במטה המשרד, באגף הבחינות ובמינהל טכנולוגיות מידע דיגיטליות, במרכז לבדיקת בחינות הבגרות והגמר (מערך המרב"ד) שמתפעלת חברה חיצונית. בדיקת השלמה בוצעה ביחידה להגנת הסייבר בממשלה (יה"ב) ובמשטרת ישראל.

הדוח שבנדון הומצא לראש הממשלה ביום 6.12.22.

מתוקף הסמכות הנתונה למבקר המדינה בסעיף 17(ג) לחוק מבקר המדינה, התשי"ח-1958 [נוסח משולב], ובשים לב לנימוקי הממשלה, לאחר היוועצות עם הגופים האמונים על

אבטחת המידע הביטחוני ובתאום עם יו"ר הכנסת, משלא התכנסה ועדת המשנה האמורה, הוחלט לפרסם דוח זה תוך הטלת חיסיון על חלקים ממנו. חלקים אלה לא יונחו על שולחן הכנסת ולא יפורסמו.

תמונת המצב העולה מן הביקורת

- **ביצוע סקר סיכונים ומבדקי חדירה ויישום תוכנית העבודה השנתית** - נכון לאוקטובר 2021, יותר משלוש שנים לאחר שביצע משרד החינוך סקר סיכונים מקיף של מערכות ליבה נבחרות שלו ומבדק חדירה בנוגע למערכת א', משרד החינוך לא ביצע סקר סיכונים מקיף ומבדקי חדירות בנוגע למערכות הליבה שלו בתדירות הנדרשת בתקנות הגנת הפרטיות אבטחת מידע - אחת ל-18 חודשים. מתוך שבע המשימות שהוגדרו ברמת סיכון "קריטית" או "גבוהה" בתוכנית העבודה לשנת 2019 של המשרד ושהמשרד קבע שיש ליישמן בשנת 2019, נכון לאוקטובר 2021, המשרד השלים את הטיפול בשלוש משימות, ובארבע המשימות הנותרות הוא טיפל חלקית.

- **מוכנות משרד החינוך להתאוששות מאסון** - משרד החינוך לא ביצע תרגילים מסוימים לשחזור מידע ולהתאוששות מאסון כנדרש בהנחיית יה"ב "גיבוי ושחזור מידע"; הוא גם לא ביצע תרגיל לשחזור מלא של מערכת מחשב מסוימת שלו.

- **עמידת משרד החינוך בחובות הנקבעות לפי תקנות הגנת הפרטיות אבטחת מידע** - עלה כי שלוש שנים לאחר כניסת תקנות הגנת הפרטיות אבטחת מידע לתוקף (במאי 2018) משרד החינוך גיבש את מסמכי מבנה המאגר, את הגדרות המאגר ואת רשימת המצאי רק עבור חמישה (10%) מ-50 מאגרי המידע שרשומים בפנקס רשם מאגרי מידע. במסמך הגדרות המאגר "תלמידים" לא עודכן מיהו הממונה על אבטחת המידע, ורשימת המצאי אינה מלאה.

- **מינוי של ממונה הגנת סייבר, כינוס ועדת היגוי סייבר והקצאת תקציב להגנת הסייבר** - מסוף שנת 2020 ועד לאוקטובר 2021 משרד החינוך לא איים את תפקיד ממונה הגנת סייבר. ועדת היגוי סייבר לא התכנסה בתדירות הנדרשת - לכל הפחות פעם בחציון. המשרד גם לא עמד בהנחיה ולפיה יש להקצות לכל הפחות 8% מתקציב תחום טכנולוגיית המידע עבור הגנת הסייבר. בפועל שיעור התקציב הייעודי שהוקצה לכך בשנת 2019 היה כ-5.66%, ובשנת 2020 הוא פחת לכ-5.06%. יצוין כי משרד החינוך מסר בתגובתו כי בחודש יוני 2022 מונתה ממונה הגנת סייבר וכי במהלך שנת 2022 (לאחר סיום הביקורת) הוא כינס פעמיים את ועדות ההיגוי לאבטחת מידע וסייבר.

- **אבטחת המידע ברשת א'** - רשת א' משרתת את כל המשתמשים שאינם עובדי משרד החינוך, ובהם בתי הספר, עובדי ההוראה, התלמידים, ההורים והספקים, והיא נגישה גם

לעובדי המשרד על פי צורכיהם. חברה א' מספקת למשרד את שירותי התשתיות המרכזיות של הרשת. להלן יפורטו עיקרי הממצאים שעלו בנוגע לרשת א':

- עלה שרכיב מסוים וגם ציוד הרשת ואבטחת המידע, הנמצא על פי חוזה ההתקשרות בטיפולה של חברה א', אינו נגיש באופן ישיר למשרד. המשרד גם אינו מבקש לקבל מהחברה דוח עיתי המפרט את ההגדרות והכללים שנקבעו לשאר ציוד הרשת ואבטחת המידע שבשליטתה, אף שהדבר נדרש כדי לוודא שההגדרות והכללים בנוגע לאבטחת המידע עומדים בדרישות המתחייבות מחוזה ההתקשרות, מצרכיו של משרד החינוך ומהנחיות יה"ב שחלות עליו.
- משרד החינוך לא ביקש אסמכתאות המתעדות את אופן הטיפול של חברה א' בקריאותיו; הוא גם אינו דורש ממנה לשלוח לו קובץ של רשומות תיעוד הפעולות (קובץ ה-log) שיאפשר לו לבצע בקרה על רשומות המתעדות את הפעולות שבוצעו במערכות.
- מערכת ה', שאמורה לאפשר ניטור של שינויים בכללי רכיבי הגנה מסוימים ובקרה עליהם, לא הוטמעה על רכיבים שבשליטת חברה א'.
- המשרד לא חיבר את רשת א' ל-SOC הממשלתי[1].

👎 **אבטחת המידע ברשת ג'** - ברשת ג' מנוהל התהליך הנוגע לבדיקתן ולהערכתן של מחברות הבחינה ששימשו את הנבחנים למענה על שאלוני הבחינה. בנוגע לרשת ג' העלתה הביקורת כלהלן:

- הרשת מוגנת על ידי גרסה מיושנת של מערכת הגנה מסוימת, שבספטמבר 2019 היצרן הפסיק לתמוך בה. נכון לנובמבר 2021 מערכת הגנה מסוימת עדכנית עדיין לא הוטמעה באופן מלא ברשת ג'.
- ברשת זו עלו פערים בנוגע לרכיבים מסוימים לאבטחת מידע.
- בינואר 2020 היצרן הפסיק לתמוך במערכת ההפעלה של שרתים מסוג מסוים שמשמשים, בין היתר, את רשת ג'.
- לרשת ג' אין רכיב שמבצע פעולת בקרה מסוימת ברמת התשתית כפי שהומלץ בהנחיות.
- שרת א' ושרתי ב' של רשת ג' אינם מופרדים; הדבר מקנה לעובדים מסוימים גישה לשרתי ב' אף שלא אמורה להיות להם גישה כזאת. בשרת א' נשמר עותק של מסד נתונים (DB) מסוים, והוא מונגש למשתמשים מורשים שניתנה להם גישה לשרת זה. יוצא כי לאותם משתמשים יש גישה גם למאגר נתונים מסוים אף שאינם מורשים לכך.

👎 **אבטחת המידע במערכת ד'** - למערכת ד' נטענים קובצי מחברות הבחינה הסרוקות וקובצי מחברות הבחינה המתוקשבות. הגישה למערכת מוקנית, באמצעות המרשתת, לכ-4,000 מעריכים חיצוניים אשר בודקים את מחברות הבחינות ומזינים עבורן ציונים. בנוגע למערכת זו העלתה הביקורת כלהלן:

- עלה כי המעריכים מתחברים למערכת באמצעות מחשבים אישיים שאינם מנוהלים

1 מרכז השליטה והבקרה הממשלתי למול איומי סייבר - Security Operation Center (להלן - ה-SOC הממשלתי).

או מוקשחים על ידי משרד החינוך וכי החיבור שלהם מאובטח חלקית.

- הפעולות הנעשות במערכת ד' נרשמות ומתועדות בקובצי ה-log, אך הן אינן מבוקרות ואינן מנוטרות.
- שישה משמונה משתמשים שתפקידם הוגדר במערכת ד' בהגדרה מסוימת, קיבלו הרשאות החורגות מתפקידם שלא על פי עקרון "הצורך לדעת"[2]; לעיתים אין זיהוי חד-ערכי של משתמשים או פירוט של הפעילות שבוצעה.
- קבצים מועברים בין מערכת ד' לבין משרד החינוך (או ספקים אחרים שלו) בלא שנבדק אם יש בהם סיכון מסוים לפגיעה אף שהתקנות מחייבות ביצוע פעולה מסוימת בעת העברת מידע ברשת הציבורית או במרשתת, יש קבצים שיש בהם מידע רגיש שמועברים ממערכת ד' למשרד בממשקים לא מאובטחים דיים, והדבר מגביר את הסיכון לדלף מידע רגיש ולפגיעה.
- במסגרת בדיקה מיוחדת שביצע משרד מבקר המדינה במערכת ד' עלה שההתקנה של צד המשתמש (לקוח - Client) וצד השרת (Server) ושבדיקת ההרשאות אינן כנדרש בהנחיות יה"ב.

אבטחת המידע במערכת ב' - מערכת ב' משמשת לרישום התלמידים הניגשים לבחינות הבגרות, כ-250 מבתי הספר מזינים באמצעותה גם את הציונים השנתיים הבית-ספריים של התלמידים (ציוני המגן). בנוגע למערכת זו עלה כלהלן:

- 64% מהמשתמשים לא נכנסו למערכת במשך קרוב לחמש שנים - בין מרץ 2017 לינואר 2022; 19% מהמשתמשים נכנסו למערכת לכל המאוחר לפני כשלוש השנים עד חמש שנים (בשנים 2017 - 2019), ורק 12% מהמשתמשים נכנסו למערכת בשנה האחרונה - ינואר 2021 עד ינואר 2022. הדבר מעורר חשש למתן הרשאות גישה למערכת לגורמים שאין להם צורך בכך.
- נכון לספטמבר 2021 משרד החינוך לא סרק במערכת הלבנה קבצים לפני העברתם לסביבה ב'. נכון לנובמבר 2021 גם החברה החיצונית לא סרקה את אותם קבצים לפני שייבאה אותם לסביבה א' או לפני שקלטה אותם במערכת ד'.

מערכת ז' שברשת ב' של משרד החינוך - משרד החינוך לא הסדיר נוהל המגדיר את שלבי תהליך עדכון ציוני הבגרות במערכת ז', את הגורמים המעורבים בו, את האחראים לכל שלב ואת הבקרה על התהליך. בפועל, עלו פערים במנגנוני הניטור והבקרה של משרד החינוך. המשרד גם לא מבצע בקרה בדיעבד - הוא לא הסדיר תהליך לקבלת דוח תקופתי קבוע המציג את הפעולות שבוצעו במערכת והמאתר פעולות החשודות כחריגות. המערכת גם לא מאפשרת בקרה פנימית בהיבט מסוים.

הפצה לא מורשית של בחינות הבגרות - בביקורת נמצאו שבע קבוצות ביישומונים להעברת מסרים מיידים הפעילות במגזר היהודי ובמגזר הערבי, שבהן התבצעה פעילות הפצה לא מורשית של שאלונים ושל הפתרונות לשאלונים. בשנים 2018 - 2020 הגיש משרד החינוך ארבע תלונות בלבד במשטרת ישראל בגין עבירת "קבלת דבר במרמה"

2 "עיקרון הצורך לדעת" - מצמצם במידת האפשר את הגורמים המורשים להיחשף לנכסי המידע הרגישים במיוחד ומקנה שקיפות בתוך המשרד בנוגע לנכסי מידע בסיווג נמוך יותר

בעקבות הפצה לא מורשית של שאלונים או של תשובות של בחינות הבגרות. ובעניין זה יצוין כי בשנת 2020 פסל המשרד יותר מ- 16,000 מחברות בחינה בשל חשד לפגיעה בטוהר הבחינות.

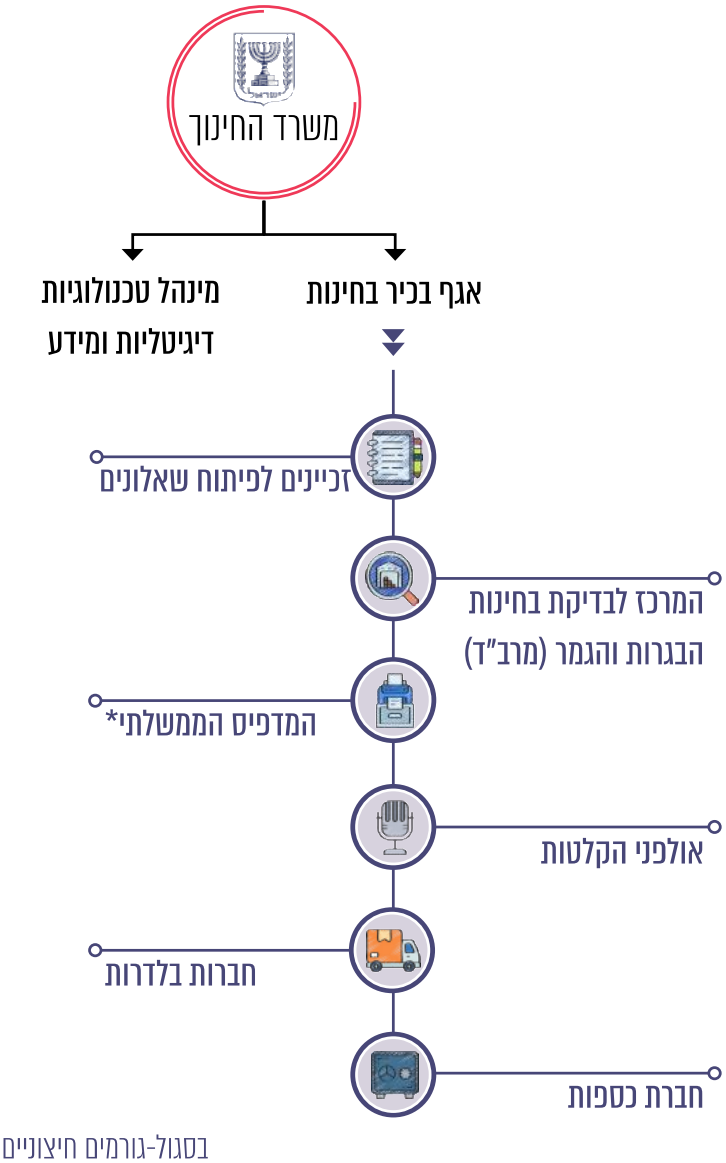
שינוי מודל של הפצת הבחינות - בשנת 2015 הקים המשרד צוות משרדי לבחינת נושא ההיערכות לבחינות הבגרות, ובשנת 2018 ביצע מיפוי וניתוח של תהליכים וסיכונים באגף הבחינות באמצעות חברה חיצונית שעמה התקשר. בעקבות כך המשרד שינה את מודל הפצת בחינות הבגרות, ובין היתר הוא רכש והתקין מאות כספות ברזל בבתי הספר שמאפשרות לו לשלוט מרחוק על שעת פתיחתן, ובהן הוא שומר את שאלוני בחינות הבגרות.

עיקרי המלצות הביקורת

- מומלץ שמשרד החינוך יקפיד על כינוס ועדת היגוי סייבר פעמיים בשנה; יישם את תוכנית העבודה השנתית במועד; יבצע סקרי סיכונים ומבדקי חדירה אחת ל-18 חודשים; יקצה לכל הפחות 8% מתקציב טכנולוגיות המידע לקידום נושא הגנת הסייבר בהתאם להחלטת הממשלה 2443 ולהנחיית יה"ב.
- מומלץ שמשרד החינוך ידרוש אסמכתאות המתעדות את טיפול חברה א' בקריאותיו, וכן מומלץ שיקבל דוחות ניטור ובקרה, דוחות של כללי רכיב הגנה מסוים והגדרות בדבר הציוד שבאחריות חברה א'. עוד מומלץ כי משרד החינוך ישקול להטמיע אמצעים שיאפשרו בקרה מסוימת לגבי אבטחת הרכיבים שנמצאים בשליטת חברה א', וכי הוא יחבר את רשת א' ל-SOC הממשלתי.
- מומלץ כי משרד החינוך יקדם את סיום ההטמעה של הגרסה המעודכנת של רכיב הגנה מסוים ברשת ג', וכי יפעל לשדרוג מערכות ההפעלה של שרתי רשת ג' שהיצרן אינו תומך בהם עוד. מומלץ שמשרד החינוך ידרוש מחברות המפעילות עבורו את מערך המרב"ד להטמיע את מערכות אבטחת המידע החסרות. עוד מומלץ שהמשרד יפעל להקמת יכולת של תיעוד ובקרה מסוימת של רשת א' ויגדיר התרעות שיאפשרו לאתר סיכוני פגיעה של הרשת.
- מומלץ שמשרד החינוך יבצע תרגילי שחזור גיבויים תקופתיים ותרגילי התאוששות מאסון. כמו כן מומלץ שיפעל לביצוע הפרדה בין שרת א' לשרתי ב' של מערכת ד'. בהיבטים מסוימים. מומלץ גם שבשרת א' לא ייעשה שימוש במסד נתונים מסוים.
- מומלץ כי המשרד יבחן מחדש את מודל החיבור של המעריכים למערכת ד' ממחשבים אישיים באמצעות חיבור מאובטח חלקית. עוד מומלץ כי המשרד יבטיח כי חברות המפעילות עבורו את מערך המרב"ד יקפידו לפעול על פי עקרון "הצורך לדעת" ולצמצם את הגישה למידע בהתאם לפרטי מידע הדרושים למשתמש לצורך ביצוע עבודתו בלבד. כמו כן, מומלץ כי המשרד יפעל לשיפור יכולות הניטור והבקרה במערכת ד'.

- מומלץ שמשרד החינוך ישלים את ההטמעה של מערכת הלבנה ברשת א' וברשת ג'. בכל הנוגע להעברת מידע רגיש בין מערכותיו לבין מערכות חיצוניות - על משרד החינוך לשפר את יכולות ההגנה מפני סיכונים המסוגלים לגרום נזק או שיבוש למערכותיו ולמידע שבהן. בהתאם לתקנות הגנת הפרטיות אבטחת מידע.
- מומלץ שמשרד החינוך יבחן את רשימת מורשי הגישה למערכת ב' ואת ההרשאות שניתנו להם. מומלץ גם שהמשרד יבצע בתדירות קבועה בקרת הרשאות בקרב משתמשי מערכת ב', בדגש על שינויים שנעשו במערך ההרשאות, ובכלל זה ישקול הטמעה של מנגנון אוטומטי לביטול הרשאות כניסה למערכת של משתמש שלא נכנס אליה במשך תקופה שתוגדר.
- מומלץ שמשרד החינוך ומשטרת ישראל יבחנו כלים להתמודדות עם תופעת ההפצה הלא מורשית של בחינות הבגרות והפצת פתרונות להן לפני שהן הסתיימו, למשל באמצעות ביצוע מעקב ובדיקות יזומות בפלטפורמות השונות שבהן מתבצעת הפצה של שאלונים ופתרונות ובכלל זה ברשתות חברתיות וביישומונים למסרים מיידיים.

הגורמים העיקריים המעורבים בתהליך הניהול והתפעול של בחינות הבגרות



בסגול-גורמים חיצוניים

על פי מידע שנאסף בביקורת, בעיבוד משרד מבקר המדינה.

* המדפיס הממשלתי הוא יחידת סמך במשרד האוצר. תפקידו העיקרי - ביצוע והפקה של עבודות הדפוס עבור משרדי הממשלה ויחידות הסמך באמצעות ייצור עצמי או באמצעות התקשרויות עם קבלני משנה חיצוניים.

סיכום

משרד החינוך אוסף, שומר ומנהל מידע רב הנוגע לבחינות הבגרות. מדובר במידע רגיש, שאבטחתו נדרשת להיות ברמה הגבוהה ביותר. בביקורת עלו כמה ליקויים בתחום אבטחת המידע - הן מתחום קיום ממשל אבטחת מידע תקין במשרד החינוך ובגופים חיצוניים שמבצעים עבורו חלק מהפעילות במיקור חוץ, והן מהתחומים הטכניים של יישום כלים, מערכות ומנגנוני אבטחת המידע והגנת הסייבר על פי הכללים שחלים עליו מתוקף תקנות הגנת הפרטיות אבטחת מידע והנחיות יה"ב.

ממצאי הדוח והבעיות שבשורש ממצאים אלה עלולים לסכן את שלמותם, זמינותם, סודיותם ואמינותם של ציוני בחינות הבגרות וכן עולה מהם חשש לפגיעה בעקרונות טוהר הבחינות. משרד מבקר המדינה ממליץ למשרד החינוך לפעול לתיקון הליקויים שהועלו בדוח, ובכלל זה לעמוד בלוחות הזמנים שנקבעו בתוכניות העבודה בתחום אבטחת המידע והגנת הסייבר, לשפר ולהעלות את רמת אבטחת המידע והגנת הסייבר בכלל מערכותיו ותשתיותיו. מומלץ גם שבמערכת החדשה לניהול ציוני הבגרות שלדברי המשרד הוא מפתח, יינתן מענה על הממצאים שהועלו בדוח זה בנוגע לאבטחת המידע של בחינות הבגרות וציוני הבגרות.