**משרד מבקר המדינה ונציב תלונות הציבור**

מכרז פומבי מס' 27/2021

### למילוי משרה פנויה

#### בלשכת המשרד בירושלים

**לשם הנוחות נוסח המכרז בלשון זכר, אולם הוא מיועד לנשים ולגברים כאחד.**

**למשרד מבקר המדינה ונציב תלונות הציבור (להלן - המשרד) דרוש/ה מנהל/ת ביקורת בתחום מערכות מידע וסייבר בלשכת המשרד בירושלים.**

**המשרה**

מנהל ביקורת בתחום מערכות מידע וסייבר.

**תיאור המשרה**

איסוף נתונים על פעולות הגופים המבוקרים ובחינת התאמת הפעולות לנורמות מחייבות בתחומים שונים; גיבוש תוכנית עבודה ממוקדת למטלת ביקורת הכוללת שלבי עבודה ולוחות זמנים, ויישום התוכנית; קיום פגישות עבודה עם בעלי תפקידים בגופים המבוקרים, ובהם בעלי תפקידים בכירים; למידה וניתוח של מידע רב, לרבות נתונים ממוחשבים, בפרק זמן קצר, תוך שימוש בכלים טכנולוגיים; ניתוח מיטבי של נושאי הדוחות והסקת מסקנות מבוססות, לשם הבטחת רמתם המקצועית של הדוחות; כתיבת דוח ביקורת רהוט, מאורגן וענייני בזמן קצוב.

**האתגרים העיקריים**

לימוד לעומק של נושאים חדשים ועיבוד חומר רב בזמן קצר; שמירה על הכשירות המקצועית, באמצעות התמקצעות מתמדת בכלים טכנולוגיים ושימוש בהם לעיבוד נתונים; יכולת הבנת תהליכים וראיית מערכת שלמה על מרכיביה השונים; התמודדות עם התנגדויות של בעלי תפקידים בגוף המבוקר, ובהם בעלי תפקידים בכירים; עבודה בצוות לצד עבודה עצמאית, לעיתים ללא הנחיה צמודה; פתיחות למשוב ולתהליכי בקרה פנימיים; עמידה בלוח זמנים מחייב; נסיעות ברחבי הארץ.

**מנהל הביקורת במבנה הארגוני**

עיקר העבודה היא עצמאית, אולם לעיתים נדרשים עבודת צוות ושיתוף פעולה עם עמיתים באגף ובמשרד. למנהל הביקורת אין כפיפים; הוא עצמו כפוף למנהל האגף ולהנחיותיו ועובד בצמידות רבה לסגן מנהל האגף.

**תנאים מוקדמים**

על המועמדים למלא אחר 2 הדרישות שלהלן במצטבר:

1. שוחררו לאחר שירות חובה מלא ביחידה טכנולוגית בצה"ל (ממר"ם, יחידת אופק 324, יחידה 8200, יחידה 3060 ומצפ"ן, חטיבת ההגנה בסייבר או יחידות מובחרות מקבילות בתחום מערכות מידע וסייבר על פי שיקול דעת המשרד) ו/או שירות ביחידת רא"ם\*.
2. בעלי ניסיון תעסוקתי של שמונה שנים לפחות - מתוכם שירות חובה מלא או שירות לאומי מלא באחת מהיחידות כאמור בסעיף א' - באחד או יותר מהתפקידים האלה: מנהל מערכות מידע, מנהל אבטחת מידע וסייבר, מנתח מערכות מידע, מנהל פרויקטי מחשוב ומערכות מידע, מפתח מערכות מידע, אנליסט נתונים (data analyst), מפתח תוכנה, ארכיטקט תוכנה, ממונה הגנת הסייבר, מיישם הגנת הסייבר, ארכיטקט הגנת הסייבר, אחראי מתודולוגיה להגנת הסייבר, מבצע בדיקות חוסן וסקרי סיכונים, חוקר סייבר. לעניין זה, ייחשב כנסיון רלוונטי גם שירות קבע של 5 שנים לפחות באחת מהיחידות המצוינות בסעיף א' בתפקידים המצויינים בסעיף ב' או המקבילים להם\*\*.

\* יש להציג אישור מגורם מוסמך על השירות ביחידה כאמור בסעיף א', לרבות ציון תקופת השירות, תקופת העיסוק ותיאור התפקיד. לחלופין, ככל שלא ניתן להציג אישור בדבר השירות ביחידות כאמור בסעיף א', יציג המועמד הצהרה בכתב לעניין זה. במקרה זה מובהר כי המשרד רשאי לפנות לגורמים המוסמכים בצה"ל או ברא"ם על מנת לאמת את הפרטים. אם הפרטים לא יאומתו המועמדות תיפסל.

\*\* יש להציג אסמכתה מהמעסיק הכוללת מידע מפורט המוכיח את הניסיון הנדרש וציון תקופת העיסוק בתחום הנדון.

\*\*\* הצגת תעודת CISA (הסמכה למבקר מערכות מידע) או CISSP או CISO או CISA/M תהיה יתרון.

**הכישורים הנדרשים**

1. כישורים בתחום הביקורת: יכולת ונכונות ללמוד תכנים חדשים ומרובים בזמן קצר; יכולת אנליטית, לשם ניתוח פריטי מידע וחומרים מרובים והסקת מסקנות מהם; כושר ביטוי גבוה בכתב, לרבות יכולת לכתוב מסמך מקצועי באופן רהוט, מאורגן, לוגי, ענייני ובשפה תקנית; כושר ביטוי גבוה בעל פה, לרבות יכולת העברת מסרים ורעיונות באופן בהיר ותמציתי; יסודיות, יכולת העמקה בפרטים, שיטתיות והפקת תוצרים מוקפדים, תוך עמידה בלוחות זמנים; יכולת התמודדות עם ריבוי נתונים ומידע ויכולת לפעול באופן מסודר ומאורגן לשם מילוי כמה משימות בו-זמנית; יכולת לפעול באופן עצמאי ללא הנחיה צמודה.
2. כישורים בתחום מערכות מידע והגנת הסייבר: ידע בתהליכי הפיתוח והתחזוקה של מערכות מידע והבקרה עליהן או בתחום הגנת הסייבר של מערכות מידע ותשתיות הארגון; היכרות עם תחום מערכות המידע, לרבות אפיון, ניתוח ומידול של צרכים ודרישות, ניתוח תהליכים, הטמעה והדרכה; בדיקה וניתוח של מחזור חיי פרויקט מערכות מידע; היכרות עם כלים ושיטות נהוגות לפיתוח, לקליטה ולהטמעה של מערכות מידע; יכולת בדיקה של מערכות מידע (ניתוח בעניין מועילות ויעילות, שלמות המידע, אמינות הנתונים, קישוריות בין מערכות, יציבות המערכות, הגנה על מידע, רציפות ותוכניות התאוששות, ממשקי המשתמש); היכרות עם תקנים והנחיות בנושא הגנת הסייבר; היכרות עם טכנולוגיות ומוצרים להגנת הסייבר;

**המשרות כרוכות בנסיעות רבות מחוץ למשרד.**