State of Israel

STATE COMPTROLLER REPORT

DECEMBER 2025

JERUSALEM

ABSTRACTS

State Comptroller Report

December 2025 | 76B

A b s t r a c t s

State of Israel

State Comptroller Report

December 2025 | 76B

Abstracts

Office of the State Comptroller | Jerusalem

Catalogue Number 2025-A-005

ISSN 0334-9713

www.mevaker.gov.il

Graphic Design: ER Design Team

Table of contents

Abstracts

Foreword

The annual audit report presented today to the Knesset addresses the examination of the defense establishment, which has a major impact on the protection of the State of Israel and its residents and the safeguarding of their security.

The report includes audits that underwent a confidentiality process in the Subcommittee of the Knesset's State Audit Affairs Committee, which decided not to present them in full to the Knesset, but rather to publish only parts of them in order to protect state security, in accordance with Section 17(a) of the State Comptroller Law, 1958 [Consolidated Version]. Below is a summary of some of the audits.

- ## Preparedness for a Terror Attack on the Light Rail in the Dan Region

  The Red Line of the light rail system was planned to serve approximately 300,000 passengers per day and is among Israel's mass transit systems, whose usage is expected to increase significantly with the addition of the two other light rail lines and the metro. The Red Line includes both underground and above-ground sections, and employs a combination of both overt and covert security and policing methods. The terror threat in Israel in general – and on the light rail in particular – intensified significantly after the surprise attack of October 7, 2023, and materialized in the attack that took place in October 2024 at the light rail station in Jaffa, which claimed the lives of seven civilians. Hence, great importance lies in the optimal preparedness of government ministries and the emergency and rescue forces for such an event, in order to save lives and minimize harm to people and property.

  The audit found that, unlike the technical and operational requirements of the Israel Fire and Rescue Authority (IFRA), which are based on binding standards, there is no legal obligation or directive requiring compliance with the technical and operational requirements of the Israel Police during the planning and tender-publication stages of transportation infrastructure projects. The audit further found that there is no established process for consultation with the designated police unit regarding preparedness for a chemical terror attack during the planning and tender-publication stages of public projects intended for mass use, such as railway stations. In addition, the Ministry of Transportation did not agree with the casualty scenario determined by the National Emergency Management Authority (NEMA) in September 2019 concerning the light rail, claiming that the projected number of casualties was too high; however, it did not present an alternative expert analysis to replace that scenario. The audit also found that even before the outbreak of the Swords of Iron War, and even more so afterward, the number of security guards employed by NTA Metropolitan Mass Transit System Ltd.

steadily decreased. Further findings revealed challenges in the evacuation of casualties; that Magen David Adom (MDA) teams operating in underground sections are not equipped with portable radios and rely on cellular phones, so that if the cellular network collapses, the teams will lack technological means of communication; that MDA communication devices are not linked to those of the other emergency services; and that no national training facility has been established for joint emergency-force drills in underground environments, despite its high importance.

The relevant bodies – the Israel Police, the Ministry of Transport, the Ministry of National Security, and the defense establishment – should act to correct the deficiencies identified by the audit, each within its respective area of responsibility. The Israel Police, the Ministry of National Security, the Ministry of Transport, and the Ministry of Finance should conduct a policy and planning process to address the shortage of security guards – a national challenge requiring urgent attention – and, upon its conclusion, take action to close the gap. It is recommended that the National Security Council (NSC), which coordinates the team tasked with establishing a training facility for the Metro Project, act to expand the training program so that it covers all underground transportation infrastructures in Israel. Additionally, the NSC should accelerate the characterization and establishment of a training facility suitable for underground environments, without waiting for the long-term Metro Project to be developed. This should be done in cooperation with other key stakeholders, such as the Ministry of Finance, the Ministry of National Security, the Ministry of Transport, the Israel Police, and the Israel Fire and Rescue Authority (IFRA).

- ## Ilan and Assaf Ramon International Airport – Elat: Airport Security against Safety Threats and Response to a Mass-Casualty Event

The Ilan and Assaf Ramon International Airport, located in the Elat region, serves as an alternative international airport to Ben-Gurion Airport. It is a critical and strategic national infrastructure facility of the highest importance. The cost of its construction was approximately 2 billion shekels, financed by the Israel Airports Authority (IAA). According to IAA data, between 2019 and 2023, the airport's operations resulted in a cumulative loss of approximately NIS 1.369 billion, representing an average annual loss of approximately NIS 274 million.

Emergency incidents at Ramon Airport or in its surrounding area may result from acts of terrorism or from a mass-casualty aviation disaster occurring at or near the airport. A mass-casualty incident (MCI) at the airport constitutes an emergency requiring the integration of resources with external emergency and rescue entities.

Due to the gaps detailed in the report regarding the response to a mass-casualty event at Ramon Airport, and given the urgency of addressing these deficiencies, the National

Security Council (NSC) should conduct a comprehensive interagency planning process in cooperation with the Ministry of National Security, the Israel Police, the Israel Defense Forces (IDF), the Ministry of Health, the Israel Airports Authority (IAA), the Ministry of Finance, and Magen David Adom (MDA). This process should aim to establish an appropriate response to emergency events at the airport and in its vicinity, including agreement on the necessary budget for its implementation. In light of the severity of the deficiencies and their impact on the airport's overall emergency preparedness, the Director of the Civil Aviation Authority should ensure that these deficiencies are remedied in order to bring the airport into full compliance with the terms of its license.

The Minister of Transportation and the Minister of National Security should ensure that Ramon Airport is fully prepared to handle emergencies. This need has become even more acute following the nature of the threats disclosed by the Hamas terror attack on October 7, 2023. Establishing a systemic response framework for Ramon Airport and its surroundings would also contribute to regulating the handling of emergencies in the city of Elat and its neighboring areas.

- ## Aspects of Oversight and Supervision by the Ministry of Defense over the Use of Marketing Agents, Representatives, and Intermediaries by Defense Companies in Defense Export Transactions

Israel's defense exports make a major contribution to its security, economic growth, and national resilience, and constitute a significant portion of the defense companies' total sales. In the years 2018–2023, Israel's defense exports amounted to approximately USD 60.5 billion. In order to increase the likelihood that business opportunities mature into actual contracts, the defense companies employ marketing agents. In the years 2022–2024, the commissions that defense companies committed to paying these marketing agents amounted to hundreds of millions of U.S. dollars.

While the activity of marketing agents may yield considerable benefits for defense companies, their use also carries significant compliance and regulatory risks concerning the potential payment of bribes to foreign public officials, as well as conflicts of interest that could lead to sub-optimal decision-making within the Ministry of Defense (MoD) and undermine equal opportunity. Materialization of such risks could also erode public trust in the public administration.

The audit revealed significant deficiencies in the Ministry of Defense's oversight and control of the use of marketing agents by defense companies. The materialization of compliance risks related to bribery and corruption could cause serious harm to the State of Israel – in terms of security, foreign relations, and international trade – as well as to the reputation of the Ministry of Defense and the defense companies involved. Accordingly, the Director General of the Ministry of Defense should ensure that the Head of the Planning Directorate and the Legal Adviser to the Defense Establishment act

promptly to formulate their recommendations regarding the level of Ministry involvement in supervising defense companies' use of marketing agents, including issues related to commissions. The Director General should then formalize the Ministry's involvement in this area within its directives. The Director General should also determine whether and how the Ministry should examine the compliance programs of defense companies and their implementation, as well as define the compliance measures that medium- and small-sized defense exporters will be required to adopt.

Given the strategic importance of defense exports and their diplomatic, security, and economic contribution on the one hand, and the risks inherent in the use of marketing agents by defense companies on the other, the Director General of the Ministry of Defense should instruct all relevant MoD entities – including the Defense Export Control Agency (DECA), the Legal Adviser to the Defense Establishment, and the Planning Directorate – to act in alignment with this report's recommendations and correct the deficiencies identified in the audit. Such measures are necessary to ensure effective oversight, which will reduce exposure to compliance and regulatory risks related to corruption and bribery in the field of defense exports.

- ## Aspects of Preventing the Leakage of Biological Pathogens and Knowledge for the Development of Biological Weapons

A biological terror event could occur if an individual or organization were to obtain a disease-causing biological agent and possess basic knowledge of its properties, methods of cultivation or preservation, and the ways it can be used to infect humans. The concern that biological weapons might be developed in various institutions during research activity, as well as concern over the leakage of pathogens or related knowledge that could be used for biological terrorism, requires the imposition of supervision and restrictions on research involving biological agents, as well as oversight of the identity of individuals participating in such research. This must be done without compromising scientific research and the important principle of publishing scientific articles based on such studies.

The audit found that the enactment of the Regulation of Research into Biological Disease Agents Law, 2008, led to the establishment of mechanisms and regulatory frameworks enabling oversight of institutions that hold biological disease agents for research purposes. However, it also found gaps in the oversight mechanisms and in the implementation of the procedures of the Committee for Regulating Research into Biological Disease Agents. The findings of this report disclose that certain provisions of the law have not been implemented, including the failure to issue regulations under it; deficiencies in the supervision of compliance with its provisions; and shortcomings in adherence to the rules governing the activity of the external institutional committee. In

addition, the findings point to partial implementation of operational procedures and of the security protocol for biological repositories in research laboratories.

At the conclusion of the audit, 16 years after the enactment of the law, the arrangements for supervising research in the field of synthetic biology had not been examined, nor had a regulatory framework been established regarding the publication of research involving biological disease agents, the dissemination of which could endanger state security, public safety, or public health. This shortcoming is particularly significant in light of the implications of using artificial intelligence (AI) tools for information retrieval and analysis. This deficiency takes on added urgency at a time when advanced technology is widely accessible and rapidly evolving, and AI tools are liable to facilitate the easy production and use of biological weapons.

It is recommended that the Ministry of Health, in coordination with the relevant government ministries, formulate regulations governing the use of synthetic biology and research involving biological disease agents that may result from such use. The gaps identified in the areas of laboratory oversight and control and the publication of dual-use biological research could increase the risk of leakage of knowledge and pathogens to criminal or hostile actors, thus enabling the perpetration of an effective biological terror attack that could harm state security, public safety, and public health.

- ## Management and Security of Databases in the Ministry of Defense

The Ministry of Defense (MoD) controls databases containing personal information, such as data on an individual's character, health status, and financial situation. The risks to privacy protection and information security in these databases have increased in the wake of the Swords of Iron War, and their materialization could impair the Ministry's ability to provide the resources required by the IDF, harm its reputation, damage its relations with suppliers and clients, and expose it to financial penalties. Moreover, such incidents could cause public alarm and a sense of insecurity, as well as harm Israel's foreign relations in security and diplomatic contexts.

In recent years, information has leaked from the Ministry of Defense, including identifying data on Ministry personnel, both as a result of cyberattacks by hostile external actors and due to human error by Ministry employees.

The findings of this audit reveal serious deficiencies in the way the Ministry of Defense manages and secures the 14 databases under its control – databases containing the personal data of approximately 2.84 million individuals. The audit found that the Directorate of Communications and Information Technology (C4I Directorate) at the Ministry of Defense, which is responsible for ensuring the Ministry's compliance with the Privacy Protection Law and the Information Security Regulations, has not mapped all the databases owned by the Ministry since 2007, has not established a procedure for

securing them, has not conducted risk assessments for databases designated as requiring a high level of security, and has not performed penetration tests of these databases' systems to assess their resilience against internal and external threats.

In addition, the report identified deficiencies in user-access management within the identity management system and the information system linked to the IDF Disabled Persons Database – a database containing information on approximately 230,000 individuals, including approximately 18,000 wounded persons whose details were added following the Swords of Iron War. The database includes information on individuals' health status, financial situation, family members, and the services provided to them. An analysis conducted by the State Comptroller's Office found that half of the external users (outsourced personnel) who had active access authorizations to the information system linked to the IDF Disabled Persons Database had not logged into the system for more than six months. 20% of these users are external consultants whose employment is managed in the Ministry of Defense's HR systems, similarly to that of the Ministry's own employees. This situation raises concern that they were granted access to the IDF Disabled Persons Database unnecessarily.

The Ministry of Defense should comply with the privacy protection requirements applicable under the Privacy Protection Law and the Information Security Regulations, particularly in light of Amendment No. 13 to the Law, which came into force in August 2025 and adapts the legislation to current challenges. In view of the findings of the data analysis conducted by the State Comptroller's Office, it is also recommended that the Ministry of Defense review its user-access management processes across all the information systems connected to its databases. It is further recommended that the Director General of the Ministry of Defense regulate the division of responsibility and authority in the field of information security for databases in the context of privacy protection, between the C4I Directorate and the Security Directorate. This is necessary to reduce risk to privacy and to fulfillment of the Ministry's mission.

- ## Preparedness for the Protection of Critical Facilities Against Missiles, Rockets, and Other Aerial Threats – Follow-up Audit

The Swords of Iron War, which broke out on October 7, 2023, underscored the heightened need of Israel's defense establishment to ensure the protection of critical facilities. In 2020, the State Comptroller's Office published an audit report on this subject, identifying significant gaps in the protection of critical facilities in certain entities, particularly those of crucial importance. Up to the outbreak of the Swords of Iron War, the Ministry of Defense, the IDF, and the National Security Council (NSC) had neither corrected any of the key deficiencies identified in the previous audit nor advanced the protection of critical facilities in the relevant entities. Even after the war began, and

despite the materialization of the aerial threats, these bodies failed to address the matter, aside from several isolated actions.

The State Comptroller draws the attention of the Ministry of Defense, the IDF, and the NSC to the failure to rectify the deficiencies identified in the previous audit and reexamined in the current one. He further points out to the NSC, the Ministry of Defense, and the Ministry of Finance that they have yet to reach agreement regarding the budgetary sources required for the protection of critical facilities in certain entities.

In light of the continued deficiencies related to the protection of critical facilities in certain entities, the Minister of Defense and the Head of the National Security Council (NSC) should jointly formulate a comprehensive policy on this matter. The Minister of Defense should instruct the Director General of the Ministry of Defense and the Chief of the General Staff to advance the mapping of the relevant critical facilities and formulate, in coordination with the relevant parties, recommendations for a multi-year work plan for their protection. This should take into account all relevant considerations, including the range of possible protective measures for these facilities and cost-benefit considerations. In addition, the Minister of Defense should define the division of authority and responsibility among the relevant entities within the defense establishment – including the National Emergency Management Authority (NEMA) and the IDF – concerning physical protection against aerial threats at critical facilities in certain entities.

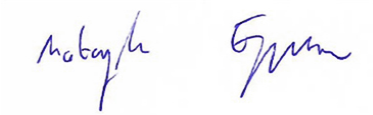
Furthermore, given the centrality and complexity of the funding issue and its importance for advancing the protection of critical facilities in certain entities, the NSC should promptly lead, in cooperation with the Ministry of Defense (which has already begun addressing the matter), the Ministry of Finance, and other relevant bodies, a planning and policy process to examine the optimal funding model for protecting these facilities, and submit its recommendations to the Security Cabinet.

It is recommended that the Prime Minister and the Minister of Defense monitor the protection of critical facilities within the specific entity and examine this issue in the other relevant entities.

The report also includes a fully classified chapter, pursuant to Section 17(c) of the State Comptroller Law, **dealing with aerial defense within the defense establishment;** hence, its contents will not be made public.

In conclusion, I wish to thank the staff of the State Comptroller's Office – both in the Defense Establishment Audit Division and in the Staff Division – for their hard work in conducting examinations and audits thoroughly, professionally, and fairly, and for publishing clear, effective, and relevant audit reports.

We continue to pray and hope for the victory of the IDF and the defense establishment, for the return for burial of all the deceased hostages, for the recovery of the wounded, and for days of peace and tranquility.



Matanyahu Englman
State Comptroller and
Ombudsman of Israel

Jerusalem, December 2025

Report of the State Comptroller of Israel |
December 2025

Chapter One

Systemic Issues

Report of the State Comptroller of Israel |
December 2025

Systemic Issues

Audit of Aerial Defense in the Defense Establishment

Audit of Aerial Defense in the Defense Establishment

An audit was conducted in the field of aerial defense in the defense establishment.

Under the authority vested in the State Comptroller in Section 17(c) of the State Comptroller's Law, 1958 [Consolidated Version], taking into account the government's rationale, after consulting with the bodies entrusted with the security of defense information, and in coordination with the Speaker of the Knesset, it was decided not to bring this report before the Knesset and not to publish it.

Report of the State Comptroller of Israel |
December 2025

Systemic Issues

Preparedness for a Terrorist Incident on the Light Rail in the Tel Aviv Metropolitan Area

Preparedness for a Terrorist Incident on the Light Rail in the Tel Aviv Metropolitan Area

Background

Metropolitan Mass Transit System Ltd. (NTA) is the entity tasked with the establishment of all mass transit systems (MTS) within the Tel Aviv Metropolitan Area. These systems encompass three light rail lines (light rail transit – LRT; light rail)[1] and three metro lines[2]. Of the three light rail lines, the Red Line was inaugurated in August 2023, while the planning process for the other two lines – the Green and Purple Lines – is still ongoing. The Red Line connects Bat Yam with Petah Tikva. It extends over a distance of 24 kilometers, of which 12 kilometers are situated within an underground tunnel, and 45 trains operate along it. Each train comprises two connected electric cars measuring 70 meters in length, with a combined capacity of 450 passengers. The frequency of the trains varies according to peak hours, averaging once every six minutes. The trains employ automatic driving mechanisms in the underground sections and manual operation in the above-ground sections.

Public transportation systems worldwide are among the preferred attack targets of terrorist groups due to their accessibility, the difficulty posed in protecting them, and the large volume of people using them. The State of Israel has endured numerous attacks on buses, and a few attacks on the light rail, within Jerusalem and the Tel Aviv Metropolitan Area. In October 2024, a deadly attack was perpetrated in the Tel Aviv Metropolitan Area, when a terrorist squad opened fire on a light rail car at one of the Red Line stations in Yafo, subsequently targeting pedestrians. In this attack, seven individuals were murdered and sixteen injured.

Unlike Israel Railways, where passengers and their belongings undergo inspection at each station, access to the Tel Aviv Metropolitan Area Light Rail, via both overhead and underground routes, is conducted in a manner akin to boarding a bus, and is subject to an overt and covert method of security and policing.

The organic security unit of the NTA and a special unit of the Israel Police are jointly responsible for the security of the Red Line during normal times and for providing immediate response in emergencies (in collaboration with teams from the "Tevel" company that operates the line). Routine security measures include the utilization of technological resources, alongside a continuous presence of security personnel at stations, as well as patrols by security guards and canine units.

1 Light rail transit is generally intended for medium-capacity passenger transport and local traffic within a metropolis. From the Encyclopedia Britannica website on the Internet.

2 The metro is an MTS infrastructure project currently being built throughout the Tel Aviv Metropolitan Area, which will facilitate future access to the Tel Aviv Metropolitan cities and the large employment centers in the country. It consists of three lines, 150 km long, and of 109 stations. From the NTA website – nta.co.il/metro/?utm_source.

Key Figures

24 km

The Red Line's track length – 12 km of which are underground, with the Red Line construction cost standing at NIS 18.8 billion

300,000 passengers per day

Passenger forecast according to NTA once the Red Line is fully operational

Approx. 800 terrorist attacks

claimed lives on public transportation in various countries around the world between 2010 and October 2019

45 trains

The Red Line includes 45 trains

5 years

have passed since the casualty scenario was determined by the National Emergency Management Authority. The Ministry of Transport disagreed with said scenario, but did not present alternative expert research on its behalf regarding this scenario

In several cases

there were fewer security guards than the standard

Challenges in evacuating casualties

Gaps were found in this area

0 portable radios are available to Magen David Adom teams

In their absence, it will be difficult for Magen David Adom (MDA) teams to communicate with each other in the event of a cell network collapse

Audit Actions

From August 2024 to January 2025, the Office of the State Comptroller examined the preparations made for a terrorist event on the Tel Aviv Metropolitan Area light rail transit. This audit was conducted at the Israel Police, the Metropolitan Mass Transit System Ltd., the Ministry of Defense, the National Emergency Management Authority (NEMA), the National Security Council (NSC), the Ministry of Transport, the National Fire and Rescue Authority (FRA), Magen David Adom (Israel's national Emergency Medical Service – MDA), the Privacy Protection Authority, and the Ministry of National Security. Additionally, site inspections were conducted along the route of the Tel Aviv Metropolitan Area light rail transit. Supplementary examinations were carried out at the Israel Security Agency (ISA). Preparedness for a terrorist event in the cyber domain are excluded from the purview of this report.

The Knesset State Audit Committee sub-committee decided not to bring this report in its entirety before the Knesset, but to publish only parts of it, for the protection of the state's security, in accordance with Section 17 of the State Comptroller's Law, 1958 [Consolidated Version].

Key Findings

The Process of Approving the Casualty Scenario in a Terrorist Incident on the Tel Aviv Metropolitan Area Light Rail – In accordance with the extreme scenario for a terrorist incident, numerous casualties are anticipated. Despite the serious threats posed to the light rail, there exists no normative resolution concerning the entity vested with the authority to determine or endorse the casualty scenario in the context of a terrorist incident on the Tel Aviv Metropolitan Area LRT. In practice, the National Emergency Management Authority established the scenario based on operational research conducted by both the Police and NTA. NEMA maintains that the Ministry of Transport should approve the casualty scenario, and the National Security Council believes that the Ministry of Transport should lead the strategic work concerning security related to transportation infrastructure projects. The audit revealed that the Ministry of Transport did not concur with the casualty scenario determined by NEMA in September 2019 for the light rail transit, on the grounds that the number of estimated casualties was too high. As of the audit end date in January 2025, five years after the establishment of the casualty scenario by NEMA, the Ministry of Transport had not presented an alternative expert assessment to justify its stance, notwithstanding its role as the body responsible for the State of Israel's transportation infrastructure and for funding its

capacity-building. It is pertinent to mention that the Israel Police informed the Office of the State Comptroller that post-October 7, it had reassessed the threat and general reference scenarios for terrorism based on threats and national reference scenarios, and had concluded that no adjustments were warranted.

- **Police Standard for Securing Mass Transit Infrastructure and Tunnel Infrastructure –** There is no legal obligation or provision mandating adherence to the technical and operational requirements set forth by the Police during the planning, initiation, and publication of tenders for transportation infrastructure projects. This is so notwithstanding that the Police serve as a legally designated guiding entity on security matters, and their approval is requisite for the opening of businesses whose operation necessitates a license. Furthermore, the Police has yet to finalize the procedures for codifying its technical and operational requirements pertaining to the underground railway environment as binding norms, despite having commenced this process in early 2023 (two years prior).

- **Preparedness for a Non-Conventional Terrorist Incident on the Red Line –** Despite the assignment of a specific unit within the defense system that bears the overall responsibility for handling incidents of chemical terrorism, and notwithstanding the real threats posed pertaining to non-conventional terror attacks, some of which have materialized in various countries, there is currently no formalized process for consulting with this designated unit in relation to preparedness for a chemical terror incident during the planning and tendering phases of public projects intended for mass use, including underground environments with enclosed spaces, such as train stations. It should be noted that adherence to the unit's recommendations is not obligatory.

- **Staffing Gaps Among Security Personnel and the Decline in their Competency Levels –** Even prior to the onset of the Swords of Iron War, and more acutely following its commencement, there has been a gradual reduction in the number of security guards employed by NTA, when in several instances, the number of security guards on duty fell below the standard, and in two cases, it was less than the minimum threshold mandated. Furthermore, refresher training for maintaining their competency, including hand-to-hand combat training not conducted during reserve service, has diminished. This degradation in the security level of Israel's mass transportation system is liable to get worse, due to the future operation of two additional Tel Aviv Metropolitan light rail lines and the metro train, leading to an increased disparity between security needs and available resources.

- **Advanced Technologies in the Red Line Security Routine –** Given that public transportation systems catering to mass transit deal with a substantial volume of passengers, the Police and NTA brought to the audit team's attention the need to explore the implementation of additional advanced technologies. While a team to evaluate the integration of such technologies was established within the metro project framework, no

corresponding team has been formed with respect to the Tel Aviv Metropolitan Area light rail project.

- **Challenges in the Evacuation of Casualties –** Gaps were found in this domain.

- **Gaps in the Means of Communication among Magen David Adom Teams in the Underground Environment –** Despite the identification of this deficiency in prior reports issued by the Office of the State Comptroller, some of which date back nearly a decade, the MDA communication system remains incompatible with the communication systems utilized by the Police and the Fire and Rescue Authority. Consequently, in the event of an incident, MDA teams will have difficulty coordinating with other emergency and rescue agencies. Additionally, MDA teams operating in underground environments are not equipped with portable radios (such devices are available solely within ambulances), relying instead on cellular phones for communication. In the case of a cellular network failure, these teams will have no way of communicating with each other through technological means, necessitating reliance on physical presence or third-party intermediaries who possess communication technology (such as police officers or fire department personnel).

- **Lack of a National Underground Training Facility for Emergency and Rescue Forces –** The initial response to a multi-casualty incident involving the light rail will be contingent upon the collaboration of rescue forces with Red Line security personnel and operators, including the Police, the Fire and Rescue Authority, and MDA. Notwithstanding the substantial importance of a national facility for training rescue forces in an underground environment, which would facilitate a simulation of all subterranean infrastructures and serve all the rescue entities, as well as the Light Rail Transit, the Home Front Command, the National Counter-Terrorism Unit (YAMAM) and others, the establishment of the facility was not advanced by all the entities recognizing its necessity, which engaged in discussions regarding the issue in 2016 in the subcommittee: the Ministry of Transport, the Ministry of National Security, the Ministry of Finance, the Police, and the Fire and Rescue Authority. As a result, from the time the issue was raised in 2016 and until the audit end date in 2025, no such facility was established, nor its construction even commenced.

Cooperation between Metropolitan Mass Transit System Ltd. (NTA) and the Police in Addressing Challenges to the Security Routine – The productive collaboration between NTA and the Police in their manner of addressing challenges to the security routine, including joint training initiatives, should be commended. These challenges have accompanied the LRT since the commencement of operations on the Red Line, and especially since the outbreak of the Swords of Iron War on October 7, 2023.

The Training and Exercise Facility where Metropolitan Mass Transit System Ltd. (NTA) Trains Security Personnel – In the event of a terrorist incident on the Red Line and prior to the arrival of rescue forces to the area, the immediate response will be based upon the personnel available and stationed along the line. The audit team conducted a visit to the training and exercise facility operated by NTA, where Red Line security guards undergo training to maintain their competency, located in Moshav Tal Shahar. The team was favorably impressed by the training and exercise programs, as well as the advanced infrastructure that enable the provision of high-quality exercises and training. Among its features is a dedicated train car designed for practicing incident response within the light rail system. It should be emphasized that this facility is not an underground training facility nor is it a national resource intended to support all rescue services; it is a ground facility designated for the training of NTA security personnel only, who are expected to deliver an immediate response to an incident occurring on the Red Line.

Key Recommendations

- The Ministry of Transport, which holds responsibility for the transportation infrastructure within the State of Israel and funds its capacity-building, must convene the parties involved in formulating the scenario for which preparations are currently underway, examine the research that informed its formulation and seek clarifications where necessary.

- Should the Ministry of Transport find the research submitted to it inadequate for establishing the reference scenario, it should initiate research efforts by its own experts on the same topic. Upon completion of this process, the Ministry should determine a casualty scenario that it is prepared to endorse and fund. Furthermore, it is recommended that the Counterterrorism and Home Front Division of the National Security Council – whose functions include serving as a regulatory and coordinative entity among all the organizations vis-à-vis the improvement of responses to terrorist threats – assist in coordinating between the Ministry of Transport, the Police, and the National Emergency Management Authority, in order to advance the ratification of a casualty scenario for the Tel Aviv Metropolitan Area Light Rail that is financially supported. The necessity of the Ministry of Transport's confirmation of the casualty scenario has gained particular significance following the October 7 attack and the subsequent intensification of security threats in the nation. It is also advised that the Police engage in regular and frequent reviews of the reference scenario, in light of the elevated security threats since October 7, and adapt its preparations accordingly. Additionally, NTA should update its preparedness in alignment with the revisions of the reference scenario established by the Police.

- To facilitate the institutionalization of the Police's technical and operational requirements document as a binding standard, it is recommended that the Police fully address the matter with the Ministry of Transport, which oversees transportation infrastructure in Israel, and

the Ministry of National Security, which oversees the Police. This should be done in order to embed these requirements as obligatory across all mass transportation projects, similar to the mandatory standard instituted for firefighting and rescue unit.

- It is advisable for the defense establishment to regulate a process concerning consultations with the designated unit regarding preparations for a chemical terrorism incident as early as the planning stages and the preparation of contractor tenders for national infrastructure projects (exhibiting characteristics similar to those of the light rail system). The defense establishment should also strive for a comprehensive framework that delineates which bodies will have the requisite authority to enforce recommendations of the bodies concerning this matter.

- The relevant stakeholders – the Police, the Ministry of National Security (which oversees the Police), and other pertinent ministries, predominantly the Ministry of Transport and the Ministry of Finance – should fully address the issue of inadequate security personnel, which poses a national challenge necessitating immediate action, and subsequently work to close the gap.

- It is recommended that the Police and NTA, with the assistance of the Ministry of Transport and the Ministry of National Security, broaden the initiatives of the technology team established at the National Security Council, so that the work encompasses references to all mass transit projects, including the Tel Aviv Metropolitan Area light rail. They should also examine measures for enhancing responses to large-scale passenger security, such as the regulation of additional advanced technologies, while maintaining an appropriate balance between privacy protection and the public interest in ensuring safety. Given that discussions on this topic are taking place in the context of the National Security Council's preparations for the metro project – anticipated to materialize only some ten years from now – it is advisable not to wait but to commence discussions at this juncture, involving the Privacy Protection Authority in the discussions concerning legal issues, thereby enabling the expedited arrangement of an additional advanced technological solution applicable to the Tel Aviv Metropolitan Area light rail system.

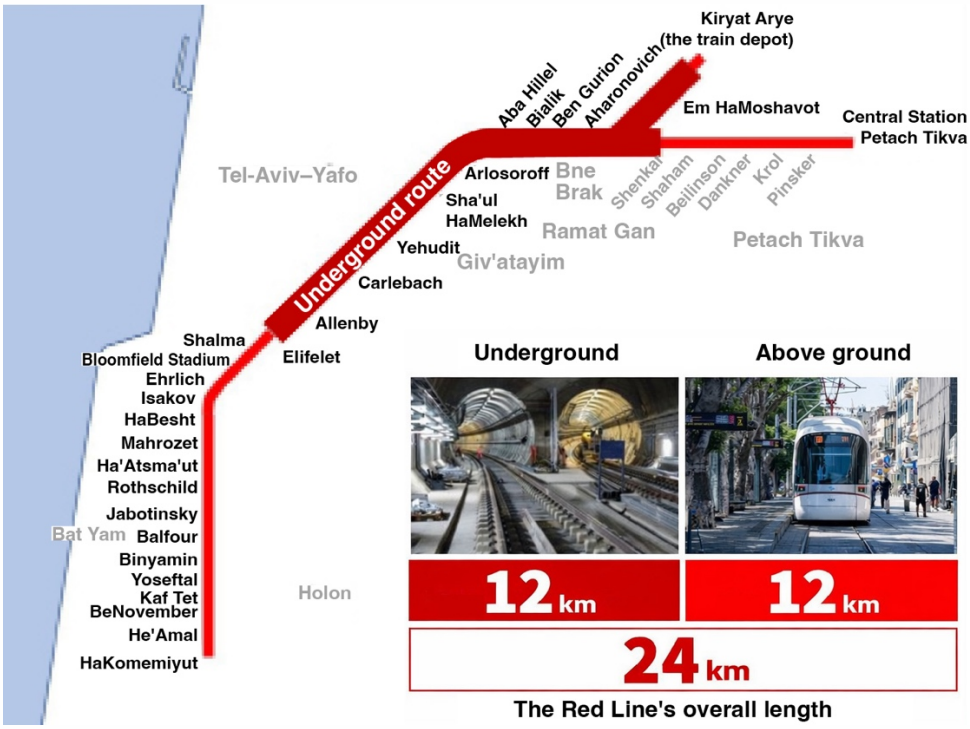
- The Police should tackle the challenges associated with the evacuation of casualties.

- The Ministry of Health, in conjunction with the Ministry of Finance, should act promptly to equip Magen David Adom with a communications system that enables effective communication among MDA teams and other rescue entities, including the Police and the Fire and Rescue Authority. MDA must ensure that its personnel are equipped with portable radios, in accordance with its multiple casualty incident doctrine, to enable communication in the underground environment of the light rail.

- It is recommended that the National Security Council, as the coordinator of the team designated with establishing a training facility for the metro project, ensure that the measures taken for conducting training are expanded to accommodate all transportation infrastructures within Israel's underground environment. This follows an identified need dating back to 2016 and not yet addressed, to enable all emergency services in Israel to

conduct simultaneous joint training exercises, underground, under field conditions approximating as far as possible those of an actual event, while ensuring resource efficiency. Additionally, it is recommended that the National Security Council expedite the characterization and establishment of this training facility for underground operations without awaiting the long-term metro project's development, as the current inability to train in such conditions may jeopardize the safety of users of the existing infrastructure. This process should be pursued in collaboration with essential stakeholders – the Ministry of Finance, the Ministry of National Security, the Ministry of Transport, the Police, and the Fire and Rescue Authority.

The Red Line Route and the Stations Along It



Source: The Metropolitan Mass Transit System Ltd. (NTA) website.

Summary

The Red Line of the light rail system was designed to accommodate approximately 300,000 passengers daily and is recognized as one of Israel's mass transit systems with an anticipated significant increase in usage due to the forthcoming addition of two additional light rail lines and a metro system. The Red Line, which features both underground and elevated routes and incorporates an overt and covert method of security and policing, is a potential target for terrorist activities. The threat of terrorism within the State of Israel escalated notably following the unexpected attack on 7 October 2023, and was manifested during the attack at the light rail station in Yafo in October 2024, which resulted in the loss of seven lives. Therefore, it is very important that government ministries, along with emergency and rescue forces, prioritize optimal early preparation for the possibility of such incidents, to safeguard human life and mitigate damage to life and property.

The audit revealed that, in contrast to the technical and operational requirements of the Fire and Rescue Authority, which are anchored in a binding standard, there exists no legal obligation or directive mandating compliance with the technical and operational requirements of the Police during the planning, initiation, and publication of tenders for transportation infrastructure projects. Additionally, there is no established regulated process for consulting with the designated unit regarding preparations for a chemical terrorism event during the planning and publishing of tenders for large-scale public projects, such as a train station. Furthermore, the Ministry of Transport did not concur with the casualty scenario set forth by the National Emergency Management Authority in September 2019 concerning the light rail, as it deemed the projected number of casualties to be excessive, while failing to present alternative expert analyses regarding this scenario. The audit further identified a persistent shortage of security personnel for the Red Line. It was also found, among other things, that challenges exist in evacuating casualties; that MDA teams in this environment lack portable radios, with the potential to impede the timely formation of a casualty overview and subsequent evacuation efforts; that the radios used by MDA teams are not connected to the communication systems of other rescue units; and that a national training facility for training all rescue personnel in underground environments has yet to be established, despite the high importance of establishing a facility of this kind.

To promote the establishment of its technical and operational requirements document as a binding standard, it is advised that the Police fully address the matter with the Ministry of Transport and the Ministry of National Security. It is recommended that the defense agencies regulate the obligation to consult with the designated unit vis-à-vis preparations for a chemical terrorism event during the planning stages of large-scale public projects, such as train stations. It is also advised that the defense agencies comprehensively regulate the entities endowed with the requisite authority for enforcing the bodies' recommendations on this issue. In the absence of a normative determination regarding the body with the authority to determine or approve casualty scenarios for terrorist events in the Tel Aviv Metropolitan Area light rail, the Ministry of Transport should convene the entities responsible for formulating the

relevant scenario, study the research relied upon in its formulation, and request clarifications as necessary. If warranted, the Ministry should initiate expert research and ultimately decide on a casualty scenario that it is prepared to fund. The Police, along with the Ministry of National Security, the Ministry of Transport, and the Ministry of Finance, should address in depth the shortage of security personnel, which presents a national challenge requiring immediate attention. Subsequently, they should take action to close this gap. Additionally, it is recommended that the Police and NTA, with the assistance of the Ministry of Transport and the Ministry of National Security, broaden the discussion of the team established within the National Security Council as part of the metro project on the topic of advanced technologies, to encompass all mass transit projects and expedite its efforts. The Police should deal with challenges associated with evacuating casualties. The Ministry of Health, in collaboration with the Ministry of Finance, should urgently equip MDA with a communication system enabling MDA teams to communicate with other rescue forces operating underground, including the Israel Police and the Fire and Rescue Authority. It is recommended that the National Security Council, as coordinator of the team designated for establishing a training facility for the metro project, ensure that the response provided for executing training is tailored to all underground transportation infrastructures within the State of Israel. It should also work to expedite the characterization and establishment of this training facility without waiting for the development of the long-term metro project, and in partnership with the stakeholders necessary for advancing the project – the Ministry of Finance, the Ministry of National Security, and the Ministry of Transport, as well as the Police and the Fire and Rescue Authority.

Accelerating the construction of the training facility will facilitate its effective utilization in conjunction with the existing light rail line and the lines that are currently under short-term development, for the training and maintenance of competencies of the rescue forces, while enhancing their ability to operate together in real time and in an optimal manner.

The audit team deems it pertinent to document its observations regarding the productive collaboration between NTA and the Police in addressing the challenges associated with security operations that have arisen since the commencement of the Red Line light rail system, especially since the outbreak of the Swords of Iron War on October 7, 2023.

Report of the State Comptroller of Israel |
December 2025

Systemic Issues

Ilan and Assaf Ramon International Airport – Elat: Protecting the Airport against Security Threats and the Response to Mass Casualty Incidents

Ilan and Assaf Ramon International Airport – Elat: Protecting the Airport against Security Threats and the Response to Mass Casualty Incidents

Background

Ilan and Assaf Ramon International Airport – Elat (Ramon Airport or the Airport) is located in the Southern Arava near Timna Park, approx. 19 km north of Elat, between Highway 90 and the Israel-Jordan border, and approx. 15 km from the Israel-Egypt border. Flight restrictions during the COVID-19 pandemic and the Iron Swords War's impact on international aviation to and from Israel, as well as on domestic aviation, have drastically reduced the airport's operation. In 2024, 658,000 travelers passed through the airport, more than 99% on domestic flights, despite an estimated potential annual passengers capacity of 2 million passengers in routine on domestic and international flights (approx. 33%).

Ramon Airport cost approx. NIS 2 billion to build, funded by the Israel Airports Authority (IAA). According to IAA figures, from 2019 to 2023, the airport lost approx. NIS 1.369 billion from operations, an average loss of approx. NIS 274 million in each of those years.

Ramon Airport is designated as an alternative to Ben-Gurion Airport. Ramon Airport is part of Israel's strategic national infrastructures.

An emergency incident at or near Ramon Airport can result from an act of terrorism or a mass aviation disaster at or near the airport. The initial response to such an emergency incident is based on the means and capabilities that are regularly in place at the airport in routine. A mass casualty incident (MCI) is an emergency incident that requires pooling resources with external rescue and emergency forces, including the Israel Police, Magen David Adom (MDA), the IDF, the Fire and Rescue Authority, the local authority, etc.

Key Figures

A short distance

The distance from the eastern fence of Ramon Airport to the border with Jordan.

A certain amount of time

The amount of time required to gather MDA and IDF medical personnel in a mass casualty incident at Ramon Airport, according to MDA procedures.

NIS 274 million

The average annual loss from the operation of Ramon Airport each year from 2019 to 2023. The total loss during these years was approx. NIS 1.4 billion. The cost of building the airport was approx. NIS 2 billion, which was funded by the Israel Airports Authority.

Audit Actions

From August 2024 to February 2025, the Office of the State Comptroller examined the protection of Ramon Airport against security threats and the response capabilities for mass casualty incidents at the airport. The audit was conducted at the IAA; the Israel Police – the security division and the operations division of the operations branch and the southern district; the Israel Security Agency (ISA); the Civil Aviation Authority (CAA); the National Security Council (NSC); the Ministry of Health; and MDA. From December 15 to 17, 2024, the Office of the State Comptroller conducted an inspection at Ramon Airport. This report is a supplementary report to a classified State Comptroller report on the protection of international civilian aviation to and from Israel that was submitted to the prime minister in January 2024, of which short sections were published in May 2024.

The subcommittee of the Knesset State Audit Committee decided not to place on the Knesset's agenda and not to publish particular data in this report for national security reasons, pursuant to section 17 of the State Comptroller Law, 1958 [Consolidated Version].

Key Findings

Coordinating the Management of Mass Casualty Incidents at Ramon Airport and the Surrounding Area

- **The Police's Command and Control in a Mass Casualty Incident –** The audit found deficiencies in this area. In addition, it was found that the Ministry of National Security had not determined the necessary budgetary source to fully address command and control issues in an emergency incident at the airport.

- **Establishing Immediate Medical Response Capabilities for Routine and Emergency Situations at the Airport –** Despite the NSC's January 2019 directive to the Ministry of Health and the Ministry of Finance; and despite the March 17, 2019, letter from the deputy director general of the Ministry of Health to the prime minister, the director of the NSC and others in which he stated that he was "announcing that the Ministry of Health will not be able to take responsibility for the medical response in routine and emergency situations at Ramon Airport"; and despite the NSC's March 28, 2019, directive, a few days after the airport opened, to quickly hold a discussion on the issue; no follow-up discussion was held at the NSC on funding a medical response plan for the airport in routine and emergency situations, and the Ministry of Health and Ministry of Finance did not decide on a budgetary source for the plan. The lack of a decision on this issue for six years, from March 2019 to the audit completion date in February 2025, is preventing the establishment of the medical response in routine and emergency situations at Ramon Airport, including mass casualty incidents. This places the passengers and others at the airport at risk.

  The audit found that there is a difference between the NSC's January 2019 directive, which is based on the Ministry of Health's July 2017 directive, which requires "the presence of a regular ambulance and a mobile intensive care unit (MICU), including staff, during the airport's hours of operation" for the immediate medical response; and the CAA director's statement at an NSC discussion in March 2025 that "the airport meets international standards, and the airport's [immediate] medical response" – "the stationing of a white ambulance + MICU with a medical clinic staffed during the airport's hours of operation by a CAA team with dual authority (medical and firefighting)" – "is sufficient."

- **The Supplementary Medical Response in Routine and Emergency Situations at the Airport –** Assembling the medical personnel in the event of a mass casualty incident at the airport is expected to take a certain amount of time. The medical response would, for the most part, not fall within the "golden hour" during which medical treatment to prevent irreparable damage to internal organs is the most effective, which could cost lives. The position of the CAA, the Israel Police, MDA, and the Ministry of Health, which

was presented at the NSC in March 2025, is that in the case of a mass casualty incident at the airport, the medical response is insufficient.

- **The Israel Police's Preparedness for a Certain Scenario –** Despite a certain Security Cabinet decision and despite the NSC's directive, the Israel Police has not yet exercised its responsibility for command and control in a certain scenario, due to certain gaps. It should be noted that the IDF made clear in its comments on a draft audit report that it is continuing to bear responsibility for this scenario until the Israel Police assumes responsibility for command and control in this scenario.

Protecting Ramon Airport

- **The Audit Found Deficiencies in the Airport's Security Arrangements in Terms of Personnel, Means, and Infrastructures.**

- **Lessons Learned in Certain Areas following the Swords of Iron War –** Deficiencies were found in this area.

- **Coordinating and Integrating Security Aspects at the Israel Airports Authority's Headquarters –** At the IAA's headquarters, there is no designated officer responsible for Coordinating and Integrating the aviation security at the airports under the IAA's responsibility, in terms of policy, development of armaments, application of technologies, and supervision and monitoring.

Ramon Airport as an Alternative to Ben-Gurion Airport

- **Ramon Airport's Capacity –** Ramon Airport can only partially function as an alternative to Ben-Gurion Airport: unlike Ben-Gurion Airport, which handles approx. 400 flights per day on average, out of which approx. 120 flights operated by Israeli airlines and approx. 280 operated by foreign airlines, Ramon Airport can only handle a maximum of 150 flights per day (approx. 38% of the number Ben-Gurion Airport handles per day). Due to Ramon Airport's limited capacity, the following guidelines have been determined: the vast majority of international flights at the airport would be those operated by Israeli airlines (approx. 120 flights per day); the number of domestic flights would be reduced to six per day; and, as a rule, cargo planes would not be handled at the airport. All of these could affect international aviation to and from Israel, as well as international trade.

Key Recommendations

- Given the risk posed by a mass casualty aviation incident and due to all of the deficiencies regarding the establishment and coordination of the handling of a mass casualty incident at Ramon Airport, the Minister of Transport and Road Safety and the Minister of National Security should ensure that the airport is prepared to handle emergency incidents, in

particular given the nature of the threats in Hamas's October 7, 2023, terrorist attack. Establishing a systemic solution for handling emergency incidents at and near Ramon Airport would also contribute to the handling of emergency incidents in Elat and the surrounding area.

- The Ministry of National Security and the Israel Police should ensure that the issue of command and control in emergency incidents at the airport is adequately addressed and funded.

- The NSC, in cooperation with the Ministry of Finance, the Ministry of Health, and MDA, should resolve the issue of allocating the funding required for the immediate medical response for mass casualty incidents at the airport, and, if necessary, bring the issue to the government for a decision; should examine the implications of the pace of assembling the medical personnel at the airport in the case of a mass casualty incident; and should ensure that the Ministry of Health and MDA are capable of exercising their responsibility to provide the medical response. Subject to the decisions made, the Ministry of Health and MDA should, without delay, complete their preparations for responding to a mass casualty incident at the airport.

- The Israel Police and the IAA should act to rectify the deficiencies found in the protection of Ramon Airport.

- Due to the deficiencies described regarding responding to a mass casualty incident at Ramon Airport and the urgency of addressing them, the NSC should perform systemic methodological preparation work in cooperation with the Ministry of National Security, the Israel Police, the IDF, the Ministry of Health, the IAA, the Ministry of Finance, and MDA, in order to ensure the provision of an adequate response to emergency incidents in and around the airport, including deciding on the required budget.

- Whereas the IAA is a statutory authority that performs actions of physical protection and handles the security of passengers at international crossings, including Ben-Gurion Airport and Ramon Airport, it is recommended that the IAA examine the need to appoint a position holder at its headquarters to be responsible for security, in order to oversee the handling of aviation security at the airports under the IAA's responsibility, in terms of policy, developing armaments, applying technologies, and supervision and monitoring.

- It is recommended that the Minister of Transport and Road Safety examine the implications of the fact that, in emergency situations, Ramon Airport can provide a partial alternative for international flights to and from Israel, and that the airport is not expected to serve as an alternative airport for cargo flights, and, accordingly, consider how to properly address these deficiencies.

Summary

Ramon Airport is an international and domestic airport located near Elat and serves as an alternative to Ben-Gurion Airport for international aviation. The airport is a critical strategic infrastructure facility of the utmost national importance.

Emergency incidents at or near Ramon Airport could result from acts of terrorism or a mass casualty aviation disaster at or near the airport. A mass casualty incident (MCI) at the airport is an emergency incident that requires pooling resources with external rescue and emergency forces. The audit found deficiencies in the Israel Police's response capabilities for mass casualty emergency incidents at the airport.

The immediate medical response plan for Ramon Airport in routine and emergency situations that has been approved by the Ministry of Health and the NSC for the scenario of a mass casualty incident at the airport has not been implemented. As a result, the medical response capabilities would not fall within the "golden hour" during which medical treatment to prevent irreparable damage to internal organs is the most effective, which could cost lives.

Due to the deficiencies mentioned regarding the response capabilities for a mass casualty incident at Ramon Airport and the urgency of addressing them, the NSC should carry out systemic methodological preparation work in cooperation with the Ministry of National Security, the Israel Police, the IDF, the Ministry of Health, the IAA, the Ministry of Finance, and MDA in order to ensure the provision of a suitable response to emergency incidents at and near the airport, including deciding on the required budget.

In his comments on the draft State Comptroller report from April 2025, the deputy director general of the Ministry of Health stated regarding the medical response to an emergency incident at the airport that "this is an issue that keeps me and the other officials at the ministry involved in this issue awake at night, while the only impediment to its resolution is a budgetary issue that is not under the responsibility of the ministry and results from a lack of funding for this after the opening of the airport was approved." In its comments on the draft audit report, the Israel Police stated that it has accepted the recommendation to conduct a systemic methodological preparation work on response capabilities for a mass casualty incident at the airport.

Given the severity of the deficiencies noted in this report on the response capabilities for a mass casualty incident at Ramon Airport, and given their impacts on the overall response capabilities for emergency incidents at the airport, the CAA's director should ensure the deficiencies are rectified so that the airport complies with the terms of its operation license.

Furthermore, the audit found that Ramon Airport can serve as an alternative to Ben-Gurion Airport for Israeli international flights and approx. 10% of the international flights operated by foreign airlines, if they continue to fly to Israel. In addition, the airport is not expected to handle cargo planes. It is recommended that the Minister of Transport and Road Safety

examine the implications of the fact that, in emergency situations, the airport can provide a partial alternative for international flights to and from Israel, and that, as an alternative airport, the airport is not expected to handle cargo planes. Accordingly, the minister should consider how to address these gaps.

Given the risk posed by a mass casualty incident, and given all of the deficiencies noted in this report, the Minister of Transport and Road Safety and the Minister of National Security should ensure that Ramon Airport is prepared to handle emergency incidents. This need is underscored by the nature of the threats in the October 7, 2023, Hamas terrorist attack. Providing a systemic solution for handling emergency incidents at and near Ramon Airport can also contribute to the handling of emergency incidents in Elat and the surrounding area.

Report of the State Comptroller of Israel |
December 2025

Systemic Issues

Aspects of Preventing the Leakage of Biological Pathogens and Knowledge for the Development of Biological Weapons

Aspects of Preventing the Leakage of Biological Pathogens and Knowledge for the Development of Biological Weapons

Background

In Israel, research groups in the medical, biological, and microbiological fields make use of biological pathogens (pathogens or disease-causing agents[1]) for research and commercial purposes. Entities in Israel that hold pathogens operate in three main sectors: government institutions (the Ministry of Health and the Ministry of Agriculture and Food Security); universities and research institutes; and the biotechnology industry[2].

A biological terrorism incident could occur, among other scenarios, if a perpetrator were to obtain a disease-causing biological agent and possess basic knowledge of its properties, its methods of cultivation or preservation, and the means by which it could be employed to achieve the objective of effectively infecting human beings with disease.

Biological security is "the set of measures intended to prevent deliberate attempts to obtain dangerous pathogens, or technologies and information that could enable the development of biological weapons. Measures of biological security include: physical protection; reporting and oversight; security in transport and transfer; personnel reliability; information security; and an integrative review of the program and the scientific research"[3]. Alongside maintaining biological security, it is important to ensure that scientific research is not compromised, nor the essential values embodied in the publication of scientific articles based on such research.

The concern over the development of biological weapons within institutions conducting medical, biological, and microbiological research, as well as the concern regarding the leakage of pathogens or knowledge related to their use for biological terrorism, necessitated the introduction of supervision and restrictions on research involving biological agents, as well as oversight of the identity of participants in such research. In order to regulate the possession of pathogens and the research activity conducted, or that could be conducted, regarding biological agents, the Knesset enacted the Regulation of Research into Biological Disease Agents, 5769-2008 (the Biological Disease Agents Research Law or the Law), whose purpose

1 Pathogens are organisms such as bacteria and fungi, as well as other disease-causing agents, such as viruses, that cause illness and challenge the body's defense systems.

2 Biotechnology is the integrative scientific activity of microbiology, biochemistry, molecular biology, and biochemical engineering, focused on the technological (industrial) application of the biological potential inherent in microorganisms, plant and animal cells, and their components, including the production of pharmaceuticals by these methods. (Hebrew University website).

3 The Israel Academy of Sciences and Humanities / National Security Council, Biotechnological Research in the Age of Terror (2008), pp. 16 and 20.

is to establish the basic arrangements for the possession of pathogens and for conducting research involving them, due to the concern of biological weapon development within institutions in the course of research, even without intent to develop such weapons. The Minister of Health is in charge of the Law's implementation and for issuing directives regarding its execution.

Key Figures

43 institutions

in the State of Israel, as of the end of the audit (November 2024), which are authorized as "recognized institutions" to hold biological pathogens or conduct research with them. These include hospitals, universities and research institutes, companies, and public health laboratories

4 biosafety levels

are set by the Work Safety Regulations[4]. The lowest is BSL-1, and the highest is BSL-4. Each laboratory is assigned the biosafety level required, according to the type of biological agent it handles

22 recognized institutions (approx. 51%)

(of the 43 existing) have not established an internal institutional committee authorized to approve the possession of pathogens and research involving them within the institution

In some of

the laboratories examined, gaps were found regarding the declaration of no prior convictions for security offenses

In a number of laboratories

deficiencies were found in conducting risk surveys

In a number of laboratories

deficiencies were found in security measures

Since 2008

when the Biological Disease Agents Research Law was enacted and until the end of the audit in November 2024, the Ministry of Health failed to issue regulations regarding the Law's implementation and the oversight of the laboratories required under it

4 Work Safety Regulations (Occupational Safety and Hygiene in Work with Hazardous Agents in Medical, Chemical, and Biological Laboratories), 2001.

Audit Actions

From August 2024 through November 2024, the State Comptroller's Office examined the oversight exercised by enforcement authorities over various research institutions (43 recognized institutions[5]), hospitals, and private companies in which research involving pathogens is conducted, or pathogens are held without research activity; the activities of several institutions operating laboratories[6]; and the advancement of the required regulation in this field. The audit was conducted in the Ministry of Health (MOH): in the Office of the Chief Scientist, in the Council for Regulating Research on Biological Pathogens, and in the External Institutional Committee; in the National Security Council (NSC); in the Ministry of Defense (MOD): in the Office of the Assistant Home Front Defense Minister; and in the Israel Police.

The audit team, through the Ministry of Health, sent questions concerning the measures taken to ensure biological security to all 43 laboratories of the recognized institutions: to four laboratories at biosafety level BSL-3 and to the remaining 39 supervised laboratories. Twenty-four of the 43 laboratories provided responses to the questions. Six laboratories replied that they do not hold biological pathogens. The other 18 laboratories addressed the questions in detail (four of them at biosafety level BSL-3 and 14 at lower biosafety levels).

The Subcommittee of the Knesset State Control Committee, in consultation with the State Comptroller, decided not to table this report in its entirety to the Knesset, and to publish only parts of it, in order to protect state security, in accordance with Section 17(a) of the State Comptroller Law, 1958 [Consolidated Version].

5 The audit team sent questions concerning the measures taken to ensure biological security to four laboratories at biosafety level BSL-3 and to the remaining 39 supervised laboratories. Twenty-four of the 43 laboratories responded to the questions, and from their responses it emerged that six of them neither hold biological pathogens (although they are recognized by the Council as institutions authorized to hold pathogens) nor engage in research in the field.

6 Belonging to recognized institutions that have been authorized to hold biological pathogens.

Key Findings

- **Issuing Regulations for Implementing the Provisions of the Biological Disease Agents Research Law –** In 2017 and 2020, the Minister of Health issued regulations pursuant to Section 24 of the Law, which governs the updating of the list of biological pathogens included in the Law's appendix7 (see Appendix A for the list of pathogens established under the Biological Disease Agents Research Law). It should be emphasized that these regulations were issued solely for the purpose of updating the list of biological pathogens, and do not address enforcement of the Law or the oversight aspects required under Section 25 of the Law. The audit found that from the enactment of the Biological Disease Agents Research Law in 2008 through the conclusion of the audit in November 2024, the Minister of Health did not issue regulations regarding the Law's implementation or the oversight of laboratories8 as required under it. Nor have regulations yet been issued establishing conditions for recognizing an institution as authorized to hold pathogens. In addition, the work rules issued by the Council for Research into Biological Disease Agents, as well as the Security Procedure for Repositories, were not anchored in formal regulations. The failure to issue such regulations may compromise the implementation of the Law and the oversight of recognized institutions, thereby increasing the risk of the leakage of knowledge and pathogens into hostile or criminal hands.

- **Assessment of Biological Security Risks in Laboratories Operating in Recognized Institutions –** The audit found that despite the importance attached to conducting risk surveys, as detailed in the Security Procedure for laboratories holding pathogenic materials published by the Council for Research into Biological Disease Agents, in some laboratories deficiencies were found in the conduct of risk survey.

- **Activity of Security Units in Recognized Institutions –** In several laboratories, deficiencies were found regarding the establishment of security procedures for laboratories.

- **Provision of Security Procedures by the Institutional Security Unit –** In several laboratories, deficiencies were found in the provision of security procedures by the institutional security unit.

- **Security Screening of Authorized Personnel –** In several laboratories, deficiencies were found in the security screening of individuals authorized for access to laboratories.

7 Biological Disease Agents Research Regulations (Amendment of the Law's Appendix), 2017; Biological Disease Agents Research Regulations (Amendment of the Law's Appendix), 2020.

8 Laboratories of recognized institutions that have been authorized to hold biological pathogens.

- **Declaration of No Security Convictions –** The audit found that in some institutions examined, deficiencies were found regarding the declaration of no prior convictions for security offenses.

- **Security and Conduct of Drills –** Deficiencies were found regarding laboratory security and the conduct of security drills.

- **Emergency Response Plans in Institutions Holding Pathogenic Materials –** Contrary to the requirements set out in the Repository Security Procedure and the rules, deficiencies were found in several laboratories in the preparation of plans for responding to emergency events.

- **Transmission of Intelligence Information to the Council for Research into Biological Disease Agents –** The Council has 15 members, including a representative from the Israel Police, the Ministry of Defense, and the National Security Council. The audit found that no arrangement exists regarding the transfer of intelligence information that may be relevant to the threat of biological terrorism or to the development and production of biological weapons related to pathogens, from representatives of the security agencies to the Council. The absence of an orderly process for transmitting intelligence information among the agencies may compromise biological security in recognized institutions. The responses of the Israel Police and the National Security Council to the draft audit report further underscored the difficulties created by the absence of such an arrangement for transferring relevant intelligence information to the Council.

- Re**gulation of Synthetic Biology –** Synthetic biology is a scientific-technological field involving the design and construction of new biological systems, elements, and components, or the redesign of existing natural biological systems for practical purposes. The Minister of Health is responsible for the implementation of the Biological Disease Agents Research Law and for issuing directives concerning its execution. The audit found that despite the conclusions of the Council for Research into Biological Disease Agents and the recognized need to examine the promotion of activity in the field of synthetic biology in Israel – including controls on the purchase and use of potentially hazardous DNA sequences, as practiced in the European Union, the United States, and Australia – the Ministry of Health took no action to regulate this field.

- **Publication of Scientific Articles That May Contribute to the Development and Production of Biological Weapons by Unauthorized Actors –** In scientific articles, the findings of studies, experiments, or reviews in a particular field are detailed, and their publication is intended to contribute to existing scientific knowledge and to share it with the global scientific community and with the public at large. The issue of biosecurity is complex, embodying the need to balance between two domains: security versus freedom of scientific research. The audit found that since 2008, the year in which the Knesset

enacted the Biological Disease Agents Research Law, the Council has not discussed the issue of regulating the publication of the findings of dual-use biological research. The audit further found that a dispute exists between the Israel Police and the National Security Council regarding responsibility for handling the security aspects involved in the publication of scientific articles concerning pathogens. The absence of oversight and control over the publication of dual-use biological research may assist hostile actors and terrorist organizations in planning and implementing an effective biological terror attack, and may harm state security, public safety, or public health. This issue assumes added significance at this time, when technology is available to nearly every person and is developing at a rapid pace. In addition, the absence of such oversight and control may enable unauthorized actors to produce and use biological weapons with greater ease.

Security Units in the Recognized Institutions – All of the recognized institutions in which the four BSL-3 laboratories operate have an institutional security unit.

Key Recommendations

- The Ministry of Health should issue regulations regarding the Law's implementation, including the procedure for submitting research applications and granting approvals, as stipulated in Section 25 of the Law, and including the method of holding pathogens and conducting research on them. It is further recommended that the Council for Research on into Biological Disease Agents assist in formulating the text of the regulations in order to advance their enactment.
- The Minister of Health should act in accordance with Section 25 of the Law, which stipulates that the Minister of Health, after consulting with the Minister of Defense, shall issue regulations establishing conditions for recognizing an institution as authorized to hold pathogens. Such consultation with the Minister of Defense is important in view of the potential security risks involved in holding pathogens, particularly when setting the rules governing the recognition of institutions authorized to hold them.
- It is recommended that the Council for monitoring research into biological disease agents also stipulate in its procedures the frequency of conducting risk surveys.
- It is recommended that the Council for Research into Biological Disease Agents establish procedures for examining the security suitability of those authorized to access biological pathogens.
- The Council for Research into Biological Disease Agents should complete the establishment of security directives for laboratories.

- The inspector at the Ministry of Health should ensure a process of drawing lessons and correcting deficiencies identified in exercises conducted in the laboratories.
- The relevant institutions should act to correct the deficiencies identified in this report.
- It is recommended that the representatives of the security agencies on the Council – the Israel Police, the Ministry of Defense, and the National Security Council – take measures to regulate the transfer of relevant intelligence information from the security agencies to the Council and establish a normative framework that determines the authority responsible for the matter, its powers, and its modes of action. In this way it will provide a solution to the disputes that exist between the Israel Police and the National Security Council.
- It is recommended that the Ministry of Health establish a regulatory framework that applies both to the use of synthetic biology and to research on pathogens that may result from its use, and coordinate this with the Ministry of Defense and other relevant government ministries. It is recommended that the Council examine the issue of publishing research on biological pathogens where there is concern that such publication could harm state security or public safety, health, or security. As part of this examination, consideration should be given to the implications of using AI tools for searching and analyzing information, and to the potential use of the information contained in research published on biological pathogens. To ensure the necessary balance between freedom of scientific research and biosecurity, the Council should also ascertain the views of the relevant academic community, as well as of the Israel Police, the Israel Security Agency (ISA or Shin Bet), the National Security Council, and the Israel Institute for Biological Research. It is recommended that the Council submit the findings of its examination to the Minister of Health and to the Knesset Science and Technology Committee and, in accordance with these findings, formulate courses of action. It is recommended that the representatives of the security agencies on the Council – the Israel Police, the Ministry of Defense, and the National Security Council – act to resolve the disagreements between the Police and the National Security Council.

Summary

A biological terrorism incident could occur, among other scenarios, if a perpetrator were to obtain a disease-causing biological agent and possess basic knowledge of its properties, its methods of cultivation or preservation, and the means by which it could be employed to achieve the objective of effectively infecting human beings with disease. The concern over the development of biological weapons in various institutions in the course of conducting research, as well as the concern over the leakage of pathogens or knowledge related to their use for purposes of biological terrorism, necessitates the imposition of supervision and restrictions on conducting research involving biological agents, as well as oversight of the identity of participants in such research. This must be done without compromising scientific research and the important values inherent in the publication of scientific articles based on such research.

The audit found that the enactment of the Biological Disease Agents Research Law, 2008, led to the establishment of mechanisms and a regulatory framework to enable oversight of institutions that hold biological pathogens for research purposes. However, it also found gaps in the oversight mechanisms and in the manner of implementing the rules set out in the procedures of the Council for Research into Biological Disease Agents. The findings of this report indicate that some provisions of the Law have not been implemented, including the failure to issue regulations under the Law, as well as gaps in oversight of the Law's implementation and in compliance with the rules governing the activity of the external institutional committee. In addition, the findings attest to only partial implementation of the work rules and the repository security procedure by research laboratories.

At the conclusion of the audit, 16 years after the enactment of the Law, arrangements regarding the oversight of research in the field of synthetic biology had still not been examined or regulated, nor had aspects concerning the publication of research on biological pathogens – where publication may pose a risk to state security or to public safety, health, or security – been regulated. This is particularly pertinent given the implications of using AI tools for searching and analyzing information. This deficiency assumes added significance in the present era, in which technology is accessible to almost anyone, is developing rapidly, and may even enable the production and use of biological weapons with relative ease through the use of artificial intelligence (AI).

It is recommended that the Ministry of Health establish regulation concerning the use of synthetic biology as well as the regulation of research on pathogens that may result from its use, and coordinate this with the relevant government ministries. The gaps identified in the performance of oversight and control of laboratories, and regarding the publication of dual-use biological research, may increase the risk of leakage of knowledge and pathogens into criminal or hostile hands, thereby assisting hostile actors and terrorist elements in planning and carrying out an effective biological terrorist attack, and causing harm to state security or to public safety, health, or security.

Report of the State Comptroller of Israel |
December 2025

Systemic Issues

Preparedness for the Protection of Critical Facilities against Missiles, Rockets, and Other Aerial Threats – Follow-up Audit

Preparedness for the Protection of Critical Facilities against Missiles, Rockets, and Other Aerial Threats – Follow-up Audit

Background

The Swords of Iron War, which broke out on October 7, 2023, illustrated the heightened need for the defense establishment to protect vital facilities. In 2020, the State Comptroller's Office published an audit report on "Preparedness for the Protection of Vital Facilities against Missiles, Rockets, and Other Aerial Threats"[1], which identified significant gaps in the protection of vital facilities in certain entities, with an emphasis on the most critical ones.

Key Figures

0 deficiencies rectified

until the outbreak of the Swords of Iron War, out of the five deficiencies examined in the follow-up audit

More than 26,000

aerial threats launched at the State of Israel from the beginning of the Swords of Iron War until early October 2024[2], from all combat arenas

14 years

elapsed since the first publication of the draft bill for handling the Home Front in Emergency Situations ("Home Front Law") until the conclusion of the follow-up audit[3]

1 State Comptroller**, Annual Report 70c** (2020), "Preparedness for the Protection of Vital Facilities against Missiles, Rockets, and Aerial Threats."

2 According to data published on the IDF website, as of October 2, 2024.

3 The Ministry of Defense attaches importance to the enactment of the law for handling the Home Front in emergency situations, among other things to define responsibility for the protection of vital facilities in certain entities against aerial threats, including their fortification.

Audit Actions

In August 2020, the State Comptroller's Office published an audit report on "Preparedness for the Protection of Vital Facilities against Missiles, Rockets, and Other Aerial Threats." The audit was conducted intermittently from September 2017 to April 2019 and examined, inter alia, the preparedness of the Ministry of Defense for the fortification of vital facilities in certain entities against aerial threats; the activity of the National Security Council (NSC) on the matter; and the legal framework for assigning responsibility for the protection of vital facilities, with emphasis on the physical fortification of these facilities and infrastructures[4].

In the months of August to December 2024, the State Comptroller's Office conducted a follow-up audit to examine the extent to which the main deficiencies identified in the previous report had been rectified. A complementary audit was carried out in January 2025. The audit was conducted, inter alia, at the Ministry of Defense: the Office of the Minister of Defense, the Office of the Director General of the Ministry of Defense the Planning Directorate the Operations, Logistics and Assets Division (EMUN), the Directorate of Production and Procurement (DOPP), and the Legal Advisor's Division (Legal Advisor to the Defense Establishment); at the National Emergency Management Authority (NEMA); at the National Security Council (NSC); and in other entities. Complementary examinations were carried out at the Ministry of Finance: the Accountant General's Department, and the Budget Department; and in the IDF.

The Subcommittee of the Knesset State Audit Affairs Committee decided not to lay this report in its entirety on the table of the Knesset, but rather to publish only parts of it, in order to safeguard state security, in accordance with Section 17 of the State Comptroller Law, 1958 [Consolidated Version].

4 It should be noted that these issues have already been addressed in previous reports of the State Comptroller, including **Annual Report 65b** (2014), in the chapter "Preparedness for the Fortification of Sensitive Facilities in the State of Israel against the Threats They Face."

Key Findings

Until the outbreak of the Swords of Iron War, the Ministry of Defense, the IDF, and the National Security Council had not rectified any of the principal deficiencies identified in the previous audit, nor had they advanced the matter of fortifying vital facilities in certain entities. Even after the war broke out, and despite the materialization of aerial threats, this matter was not advanced, aside from a few isolated actions.

The State Comptroller brings to the attention of the Ministry of Defense, the IDF, and the National Security Council their failure to rectify the deficiencies identified in the previous audit and examined in the course of this review.

Activity of the Defense Establishment for Fortifying Vital Facilities in Certain Entities – The previous audit found that staff work for mapping certain vital facilities in certain entities had not yet been completed: the Ministry of Defense had not determined which infrastructures in these entities required protection, had not prepared for their fortification, and did not possess a work plan for carrying it out, including its budgeting.

1. **The follow-up audit Found that until the outbreak of the Swords of Iron War, this deficiency had not been rectified:**

   - The Ministry of Defense had not mapped the vital facilities that required fortification and, accordingly, had not prepared a multi-year work plan for their fortification, despite the risk of their being vulnerable to aerial threats possessed by the enemy on a broad scale.

   - The IDF had not presented the Ministry of Defense with certain information required in order to advance the matter. Repeated appeals by a particular entity to the Ministers of Defense in the years 2019–2022 – regarding the need to promote solutions for fortifying its critical facilities, including the allocation of resources – went unanswered, and the Ministry of Defense did not act to provide a response, leaving the entity with significant fortification gaps.

2. **The follow-up audit found that after the outbreak of the Swords of Iron War, the deficiency was rectified to a minor extent:**

   - The Ministry of Defense and the IDF did not carry out joint work aimed at defining vital facilities in certain entities.

   - The Ministry of Defense did not map the vital facilities requiring fortification in certain entities, nor did it prepare a multi-year work plan for their fortification, including its budgeting. This was apart from the Ministry of Defense's

involvement in promoting a proposal to finance a fortification program for vital facilities in a particular entity, and from specific fortification measures – actions that do not substitute for the necessary staff work required for the physical fortification of vital facilities in certain entities. It was only in December 2024, at the conclusion of the follow-up audit, that the Director General of the Ministry of Defense instructed the establishment of a team to address the fortification of vital facilities.

- **A Program for Fortifying and Ensuring Redundancy of Vital Facilities in a Particular Entity**

  - Following the Prime Minister's directive to the head of the National Security Council (NSC) to discuss the fortification program for a particular entity, the NSC held deliberations on the matter. The follow-up audit found that pursuant to the Prime Minister's directive of November 2023, in June 2024 the head of the NSC instructed the Ministry of Defense to submit its comments on the draft opinion regarding this entity's fortification program by July 2024. Only in January 2025, at the time of the completion of the follow-up audit and approximately six months after the requested deadline, did the Ministry of Defense convey its opinion to the NSC.

  - As of the completion of the audit (January 2025), the NSC and the Ministry of Defense had not finalized the fortification program for the entity in question, including its budgeting.

- **Division of Authority and Responsibility Regarding the Fortification of Vital Facilities in Certain Entities among Defense Establishment Bodies –** The audit found that in the period between January 2019 and the conclusion of the follow-up audit (December 2024), authority and responsibility for fortifying these facilities shifted among several bodies within the Ministry of Defense. However, during this period, the Directorate of Production and Procurement (DOPP), the Planning Directorate, and the National Emergency Management Authority (NEMA) did not act to fulfill their responsibility in this matter. Moreover, these bodies do not view themselves as responsible for the matter and consequently failed to advance it. This gap resulted in the absence of decisions on the matter and in its lack of progress.

- **Involvement of the National Security Council in the Protection of Vital Facilities in Certain Entities –** In the previous audit, it was found that the National Security Council (NSC) had not proposed to the Prime Minister topics for discussion at meetings of the Ministerial Committee for Home Front Emergency Preparedness during its tenure, or at meetings of the Security Cabinet, regarding the existence and quality of the activity of the relevant bodies for the protection of vital facilities in certain entities, including their physical fortification where necessary, as well as the timeframes and

budgets required for this purpose. This was despite the provisions of the NSC Law and notwithstanding the national importance of these infrastructures.

1. **The follow-up audit found that until the outbreak of the Swords of Iron War, this deficiency had not been rectified**

   - From the conclusion of the previous audit (April 2019) until the outbreak of the Swords of Iron War, the NSC – serving as the body that coordinates the staff work of the government, the Security Cabinet, and all other ministerial committees on foreign and security matters, and that proposes to the Prime Minister the agenda and issues for discussion in the Security Cabinet – did not propose to the Prime Minister to bring to the Security Cabinet's attention the preparedness of the relevant bodies for the protection of vital facilities in certain entities, including their physical fortification where necessary. Consequently, the matter was not discussed at the Security Cabinet's meetings, despite the national importance of these facilities and despite the State Comptroller's recommendation in the previous report.

   - Although it was understood that air defense systems do not provide a hermetic solution, and although the NSC did participate in activities related to the fortification of some vital facilities, it did not address the physical fortification of other critical facilities until the outbreak of the Swords of Iron War, during which the aerial threats materialized.

2. **The follow-up audit found that after the outbreak of the Swords of Iron War, the deficiency was rectified to a minor extent –** Only after the outbreak of the Swords of Iron War, during which the aerial threat to vital facilities materialized, and following the Prime Minister's intervention in the matter and the approach of a particular entity to the Head of the NSC in December 2023, did the NSC for the first time hold a dedicated discussion on the fortification of vital facilities. However, no framework for advancing the issue has yet been determined. The follow-up audit further found that despite the occurrence of significant aerial threats during the war, as of the audit's conclusion the NSC had not completed a comprehensive examination of the need to fortify vital facilities in certain entities and had not proposed to the Prime Minister that the issue be brought before the Security Cabinet.

Funding Sources for Implementing a Fortification Program – The previous audit found that the Ministry of Defense did not have a work plan for fortifying vital facilities, including budgeting. The follow-up audit found that this deficiency **had not been rectified:**

- As of the audit's conclusion in December 2024, the Ministry of Defense had not taken measures to find a solution to the funding issue, including raising the matter before the government, as recommended by the State Comptroller in the previous report. This was despite recognition of the importance of vital facilities in certain

entities, the tangible risks of harm from aerial threats, and the understanding that fortification costs are high and require agreed funding sources.

- Despite the NSC's instruction to the Ministry of Defense to carry out staff work and establish a unified policy, including clear criteria, for the state's participation in funding future requests for the fortification of facilities in certain entities, the Ministry of Defense did not undertake the required work. Accordingly, as of the audit's conclusion in December 2024, and a year after a particular entity's inquiry regarding the fortification program of a certain body, no decision had been reached concerning the program or its funding.

- The follow-up audit found that the NSC, the Ministry of Defense, the Ministry of Finance, and a certain regulatory body had not yet reached agreement on the budgetary source for financing the fortification of vital facilities in certain entities, and that each body had in mind a different solution to the funding issue. The Ministry of Defense's position is that its budget does not contain the resources required for fortifying certain entities. The position of the Accountant General's Division and the Budget Department at the Ministry of Finance is that the financing should come from the resources of certain entities or be drawn from the Ministry of Defense's budget.

Normative Regulation of the Fortification of Vital Facilities in Certain Entities through Legislation – The previous audit found that as early as February 2011 the Ministry of Defense introduced the draft Home Front Emergency Bill, 2011[5], but as of the conclusion of the previous audit, in April 2019, the government had neither discussed nor approved the draft. The follow-up audit found that the deficiency **has not been rectified:** Despite the importance the Ministry of Defense attaches to the enactment of the Home Front Emergency Law – inter alia for establishing responsibility for the protection of vital facilities in certain entities against aerial threats, including their fortification – and despite the passage of approximately 14 years since the draft bill was first introduced, as of the conclusion of the follow-up audit (December 2024) the draft bill was still at a preliminary stage, with no anticipated end date for the legislative process.

Normative Regulation of the Fortification of Vital Facilities in Certain Entities by Means of a Government Decision – The previous audit found that NEMA had not yet submitted to the Ministerial Committee for Home Front Preparedness for Emergencies or to the Security Cabinet a draft government decision establishing, inter alia, a mechanism for exempting certain vital facilities from the list; nor had the inter-ministerial

5 The name of the bill at the conclusion of the audit was "Civilian Preparedness for Emergencies in the Economy".

committee[6] or NEMA submitted the consolidated list of vital facilities, including certain facilities, to the Ministerial Committee for Home Front Preparedness for Emergencies during its tenure, or to the Security Cabinet and the government for their approval. The follow-up audit found that the deficiency **has not been rectified:** despite the existence of a 2011 government decision on the protection of critical national infrastructures and sensitive facilities in Israel, which, among other things, established an inter-ministerial committee to address the matter – with the participation of many actors, including representatives of the relevant government ministries, the IDF, the Ministry of Defense, and the NSC – there is no parallel government decision establishing a similar mechanism for addressing certain vital facilities, and these facilities were not included under any government decision. This is so despite the fact that the Director General of the Ministry of Defense and another source noted the need for such regulation. The absence of normative regulation in this matter, including by means of a government decision, may result in the failure to advance the fortification of vital facilities in certain entities.

Key Recommendations

- The Minister of Defense should instruct the Director General of the Ministry of Defense and the IDF Chief of Staff to advance the mapping of vital facilities and to formulate a recommendation for a multi-year work plan for their fortification, taking into account all relevant considerations, including the range of possible measures for their protection, as well as cost-benefit considerations.
- The Minister of Defense should define the division of authority and responsibility among defense establishment bodies – including NEMA and the IDF – regarding the physical fortification of vital facilities in certain entities against aerial threats, and should instruct that these definitions be reflected in the directives of the bodies.
- The Head of the NSC and the Minister of Defense should instruct the completion and implementation of a fortification program for a particular entity, as well as a joint review of the fortification needs of vital facilities in the other relevant entities.
- The Head of the NSC should bring before the Prime Minister, as soon as possible and as a subject for discussion at the meetings of the Security Cabinet, the issue of fortifying vital facilities in certain entities, for the purpose of formulating comprehensive policy on the matter.
- The NSC should promptly lead, together with the Ministry of Defense – which has begun to address the matter – the Ministry of Finance, and other relevant parties, a thorough examination of the optimal funding model for fortifying vital facilities in certain entities, and

6 An interministerial committee headed by the Director of the National Emergency Authority (NEMA) tasked with determining the criteria for types of facilities, assessing risks, and setting national-level priorities.

should present its recommendation to the Security Cabinet. This is in view of the centrality and complexity of the funding issue and its importance for advancing the fortification of these facilities. It is also due to the urgent need to accelerate fortification plans of these facilities in light of the significant aerial threats they face. It also follows the Prime Minister's directive that the Head of the NSC convene a discussion on the fortification and redundancy plan of a particular entity. The State Comptroller stresses that this requires an inter-ministerial effort, which is a necessary condition for advancing the matter.

- Given that approximately 14 years have passed since the initial introduction of the Home Front Emergency Bill – due, among other things, to the complexity of the issue, the involvement of many stakeholders, and the financial burden the law imposes on the entities concerned – the Minister of Defense should delve into the matter and instruct that a course of action for further advancing the bill be examined, while addressing the reservations raised by various parties that have delayed its enactment to date.

- In view of the significant aerial threats facing certain entities and the national strategic need for their fortification, it is recommended that the Minister of Defense, in coordination with the NSC, bring the issue of regulating the physical fortification of vital facilities in certain entities before the Security Cabinet for its decision.

- It is recommended that the Prime Minister monitor the implementation of his directive concerning the fortification of a particular entity and consider fortification of the other relevant entities.

Summary

The previous audit found that for many years there have been significant deficiencies in the activity of the Ministry of Defense, the IDF, NEMA, and the NSC – each in its own domain – with respect to the protection of vital facilities. The follow-up audit found that despite a significant increase in aerial threats since the publication of the previous report, until the Swords of Iron War none of the five deficiencies examined as part of the follow-up audit had been rectified. During the war, 40% of these deficiencies were rectified to a minor extent, while the remainder were not rectified at all.

With the outbreak of the Swords of Iron War, the risk of harm to vital facilities in certain entities increased. Nevertheless, the Minister of Defense and the Director General of the Ministry of Defense did not take measures, up to the conclusion of the audit (January 2025), to advance the fortification of vital facilities. Their actions were limited to isolated measures and to the Director General's directive, issued in December 2024 (more than a year after the outbreak of the war and at the conclusion of the follow-up audit), to establish a team to address the matter. Similarly, the NSC failed to complete a comprehensive examination of the need for fortifying the vital facilities of certain entities, nor did it propose to the Prime Minister to bring the matter to the attention of the Security Cabinet.

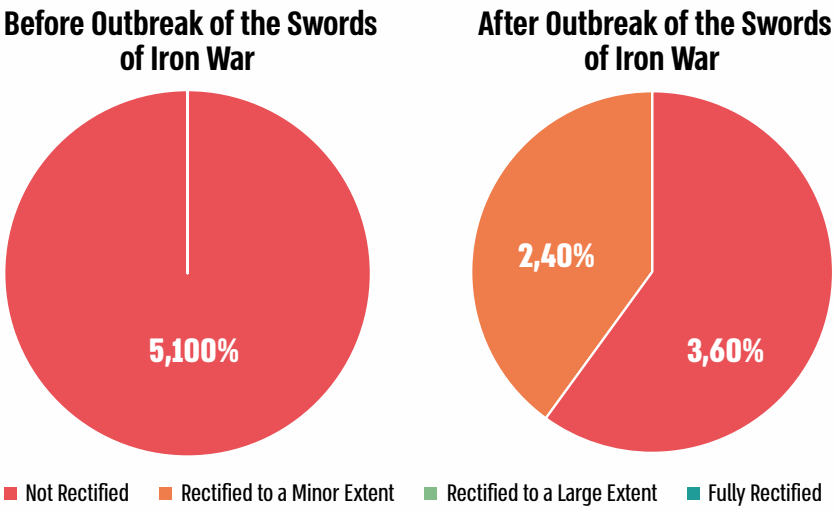
The State Comptroller points out to the Ministry of Defense, the IDF, and the NSC their failure to rectify the deficiencies identified in the previous audit and re-examined in this audit, and further notes that the NSC, the Ministry of Defense, and the Ministry of Finance have not reached agreement regarding the budgetary sources for the fortification of vital facilities in certain entities.

In view of the persisting deficiencies in the fortification of vital facilities in certain entities, the Minister of Defense and the Head of the NSC should work jointly to formulate a comprehensive policy on the fortification of such facilities. The Minister of Defense should instruct the Director General of the Ministry of Defense and the Chief of Staff to promote the mapping of these vital facilities and, in collaboration with relevant actors, develop a recommendation for a multi-year work plan for their fortification where required. This should take into account the full range of considerations, including the various possible means of protecting these facilities and cost-benefit considerations. The Minister of Defense should also define the division of authority and responsibility among defense establishment bodies, including NEMA and the IDF, regarding physical fortification against aerial threats to the vital facilities of certain entities.

In addition, given the centrality and complexity of the funding issue and its importance for advancing the fortification of the vital facilities in certain entities, the NSC should promptly lead, together with the Ministry of Defense (which has already begun to address the matter), the Ministry of Finance, and other relevant actors, a thorough examination of the optimal funding model for the fortification of these facilities, and submit its recommendation on the matter to the Security Cabinet.

It is recommended that the Prime Minister and the Minister of Defense monitor the fortification of the vital facilities of a particular entity and examine this issue with respect to other relevant entities as well.

Main Deficiencies Raised in the Previous Report, by Extent of Rectification



Extent of Rectification of the Main Deficiencies Raised in the Previous Report

Audit Chapter	Audited Body	Deficiency Noted in Previous Audit	Extent of Rectification of Deficiency as Found in Follow-up Audit			
			Not Rectified	Rectified to a Minor Extent	Rectified to a Large Extent	Fully Rectifie
Defense Establishment Activity to Advance the Fortification of Vital Facilities in Certain Entities Prior to the Outbreak of the Swords of Iron War	Ministry of Defense, IDF	The staff work for mapping vital facilities in certain entities had not yet been completed: The Ministry of Defense had not yet determined which vital facilities required protection, and had not prepared for their fortification				
Defense Establishment Activity to Advance the Fortification of Vital Facilities in Certain Entities Following the Outbreak of the Swords of Iron War						

Audit Chapter	Audited Body	Deficiency Noted in Previous Audit	Extent of Rectification of Deficiency as Found in Follow-up Audit			
			Not Rectified	Rectified to a Minor Extent	Rectified to a Large Extent	Fully Rectifie
NSC Involvement in the Fortification of Vital Facilities in Certain Entities up to the Outbreak of the Swords of Iron War	NSC	The NSC did not propose to the Prime Minister topics for discussion in meetings of the Ministerial Committee for Home Front Emergency Preparedness during its tenure, or in meetings of the Security Cabinet, concerning the existence and nature of the activities of the relevant actors in protecting vital facilities in certain entities – including, where necessary, their physical fortification, the timeframes, and the required budget. This was despite the provisions of the NSC Law and the national importance of these infrastructures				
NSC Involvement in the Fortification of Vital Facilities in Certain Entities Since the Outbreak of the Swords of Iron War						
Funding Sources for the Implementation of a Fortification Program for Vital Facilities in Certain Entities	Ministry of Defense	The Ministry of Defense does not have a work plan for fortifying vital facilities in certain entities, including its funding				

Audit Chapter	Audited Body	Deficiency Noted in Previous Audit	Extent of Rectification of Deficiency as Found in Follow-up Audit			
			Not Rectified	Rectified to a Minor Extent	Rectified to a Large Extent	Fully Rectifie
Normative Regulation through the "Home Front Emergency Law	Ministry of Defense	As early as February 2011, the Ministry of Defense introduced the Home Front Emergency Bill, but as of the conclusion of the previous audit (April 2019), the government had not yet discussed or approved it	➡			
Normative Regulation through a Government Decision	Ministry of Defense	NEMA had not yet submitted to the committee and to the Security Cabinet a draft government decision establishing, among other things, a mechanism for exempting certain vital facilities from the list[7]; nor had the inter-ministerial committee or NEMA submitted the consolidated list of vital facilities to the Ministerial Committee for Home Front Emergency Preparedness during its tenure, or to the Security Cabinet and the government, for their approval	➡			

7 A list of sensitive civilian facilities and infrastructure complexes requiring protection, including through physical fortification.

Report of the State Comptroller of Israel |
December 2025

Chapter Two

Ministry of Defense

Report of the State Comptroller of Israel |
December 2025

Ministry of Defense

Management and Security of Databases in the Ministry of Defense

Management and Security of Databases in the Ministry of Defense

Background

The Ministry of Defense plays a central role in achieving the State of Israel's national security objectives and, in carrying out its missions, makes use of extensive databases, including those of employees, suppliers, clients, Israel Defense Forces (IDF) disabled veterans, bereaved families, IDF casualties, freed hostages, and consultants. These databases contain personal data, such as data on an individual's character, personal status, health condition, financial status, and professional qualifications. Disclosure of the data from these databases could infringe on the right to privacy of the individuals whose sensitive information is stored in them, a right that is among the most important human rights in Israel. In addition, such disclosure could have implications for the functioning of the Ministry of Defense and for state security, as described below.

Possible Implications Resulting from the Disclosure or Disruption of the Ministry of Defense's Databases

The Individual
- Loss of ability to exercise rights
- Prevention of access to services or opportunities
- Loss of control over personal data usage
- Identity theft
- Financial loss
- Reputational damage
- Breach of confidentiality
- Discrimination

Ministry of Defense
- Impairment of the Ministry of Defense's normal operations and its ability to perform its role in achieving the State of Israel's national security objectives
- Damage to reputation and erosion of public trust
- Damage to relationships with suppliers and clients
- Exposure to legal claims, financial penalties, and high compensation payments

National Security
- Psychological impact: sowing panic and a sense of insecurity
- Damage to foreign relations in security and diplomatic contexts
- Harm to the State of Israel's vital systems

The risks to privacy protection and to data security in the Ministry of Defense's databases have increased since the outbreak of the Swords of Iron War, in light of the intensification of

cyberattacks, which are an integral part of modern warfare. These have included attacks on the databases of public bodies and an increase in phishing attempts targeting entities in Israel, including former members of the defense establishment. Such attempts have become more sophisticated and more focused on the target, by gathering preliminary information regarding the target's occupation and fields of interest. In 2024, there was a 24% increase in the number of cyber incidents verified by the Israel National Cyber Directorate compared with 2023 (17,078 cyber incidents in 2024, compared with 13,040 in 2023). The most common attacks were phishing incidents: in 2024, 10,084 such incidents were verified, compared with 3,301 in 2023; 44% of phishing incidents in 2023 (1,449 incidents) occurred from October 7 through the end of 2023. In addition, 1,771 incidents of intrusion into computer systems were verified in 2024, compared with 1,714 in 2023; half of these incidents in 2023 (873) occurred from October 7 through the end of that year.

The materialization of the risks to the Ministry of Defense's databases could, for example, result in the disclosure of personal data about soldiers injured in the war (the database of IDF disabled veterans) or about former hostages from the October 7 massacre who were released from Gaza (the database of freed hostages) and who, against their will, became subjects of public interest. In addition, disclosure or disruption of information from security-importance databases – such as the Ministry of Defense employee database and the Ministry's supplier database, whose confidentiality must be maintained – could impair the Ministry's functional continuity and its ability to provide the Israel Defense Forces with the required means, cause it reputational damage, harm its relations with suppliers and clients, and expose it to fines. Moreover, this matter carries psychological implications: it could even sow panic and a sense of insecurity among the public, and harm Israel's foreign relations in security and diplomatic contexts.

Indeed, since the outbreak of the Swords of Iron War, the risk of a data leak from the Ministry of Defense has materialized: in April 2024, the media reported that data from the Ministry of Defense's administrative portals had been leaked by hostile actors and published on a website established by international hackers. This included identifying information on Ministry employees, information on defense tenders, and on Israel Defense Forces technological systems, such as details about armored vehicles, engineering blueprints, and technical information on satellite imaging systems.

Key Figures

14

The number of databases containing personal data[1] registered by the Ministry of Defense in the Database Public Registry; 8 of which (57%) are subject to a high level of security due to the security risks they pose

2.84 million people

contained in the Ministry of Defense's databases containing personal data, including 230,000 individuals whose details are listed in the IDF Disabled Veterans database, which holds data on their health and economic status, their family members, the services provided to them, etc., 18,000 of them injured in the Swords of Iron War

18 years have passed

since the Ministry of Defense last conducted a comprehensive mapping of all the databases it controls (2007), to determine whether it was subject to additional requirements under the Privacy Protection Law; hence, it may control additional databases

0

The number of risk assessment surveys conducted by the Ministry of Defense to identify data security risks in the databases, and the number of penetration tests to database systems carried out to protect them from external and internal threats

Up to NIS 320,000

The amount of the administrative financial fine for each high-security-level database to which the Ministry of Defense could be exposed for failing to conduct risk assessment surveys and penetration tests, upon the entry into force of Amendment No. 13 to the Privacy Protection Law

7 out of 10

external users[2] with access authorization to the Ministry of Defense's central computer network had not logged into the network for more than six months; 60% of them had not logged in at all. 90% are outsourced workers. Accordingly, there is a risk that they hold network access authorization without need

60%

of the external users who had not logged into the network for more than six months are affiliated with five Ministry of Defense departments, where the risk of exposure of security-related information, or information regarding individuals is high

5 out of 10

external users with access authorization to the database system managing the IDF Disabled Veterans database had not accessed the system for more than six months. Accordingly, there is a risk that they hold access authorization to the database without need

1 Such as information on an individual's personality traits, personal status, health condition, financial status, and professional qualifications.

2 The Ministry of Defense's computer systems users are divided into two groups: (a) Internal users – users whose personal details are managed in the Ministry of Defense's human resources systems, including Ministry employees, consultants, national service volunteers, and Israel Defense Forces soldiers serving in the Ministry; (b) External users – users whose personal details are not managed in the Ministry's human resources systems, including outsourced workers, employees of defense industries, and IDF users.

Audit Actions

From August 2024 to January 2025, the State Comptroller's Office examined how the Ministry of Defense manages the databases under its control and how it secures them, in light of the provisions of the Privacy Protection Law, 1981, and the Privacy Protection Regulations (Data Security), 2017. It should be noted that the audit did not address the cyber aspects of information security. The audit was conducted in the Ministry of Defense – in the Applications and Technology Department ("the Applications and Technology Department") and the Security Department; in the Ministry of Justice – in the Privacy Protection Authority. Supplementary examinations were conducted in the Rehabilitation Department of the Ministry of Defense.

It should be noted that since Amendment No. 13 to the Privacy Protection Law will enter into force in August 2025, after the audit's completion date, the Ministry of Defense's activity was examined according to the provisions of the Law prior to the amendment, and in alignment with the requirements that will apply to it on a forward-looking basis. Accordingly, the definitions, terms, and recommendations presented in this report with respect to the Privacy Protection Law and the Privacy Protection Regulations (Data Security) are consistent with Amendment No. 13 to the Law.

Key Findings

Compliance of the Ministry of Defense with Requirements for Data Security in Databases (Privacy Protection Aspects) – The Ministry of Defense's Applications and Technology Department has not fulfilled its responsibility to ensure compliance with the privacy protection requirements applicable to the Ministry regarding data security in its databases. These requirements include establishing a data security procedure, conducting risk assessment surveys, penetration tests and training sessions to raise employee awareness. Instead, the Applications and Technology Department has relied on the Security Department, which is the professional authority for data security in the Ministry, without verifying that the actions taken by the Security Department address all the unique requirements relating to privacy protection. It should be noted that the Security Department does implement measures for securing information; however, these measures are intended to secure classified information as defined in the Regulation of Security in Public Bodies Law, 1998, under which the Department operates, and they do not fully address data security requirements for databases from a privacy protection perspective.

Failure to comply with the data security requirements prescribed in the Privacy Protection Regulations increases the risks to the databases, including data leaks, data disruptions and impairment of its availability, particularly given the unique challenges of enforcing privacy protection in computerized databases. In recent years, data has leaked from the Ministry of Defense both as a result of cyberattacks by hostile external actors, who exfiltrated data from the Ministry's administrative portals – including Ministry employees' identifying data, details of defense tenders, and information on Israel Defense Forces technological systems such as engineering blueprints and technical data[3]; and as a result of human error on the part of employees who inadvertently published ID numbers, names, and vehicle registration numbers of senior Ministry of Defense officials[4].

- **The Supervision of the Ministry of Defense on the Implementation of the Privacy Protection Regulations (Data Security) in Its Databases** – Contrary to the requirements of the Privacy Protection Law and its Regulations, according to which a Data Security Officer of databases will be appointed and will regularly monitor the compliance with Data Security Regulations, there is no position within the Ministry of Defense tasked with identifying the requirements applicable to the Ministry under the Law and the Regulations, validating compliance with them, and supervising their implementation. Furthermore, up until October 2024, the Head of the Applications and Technology Department of the Ministry of Defense – who is tasked with managing the Ministry's databases and, by law, bears direct responsibility for the security of the data in them as well as for meeting the obligations outlined in the Regulations regarding the databases controlled by the Ministry – did not ensure that the Data Security Officer fulfilled her duties as required by the Regulations. Consequently, he did not monitor the Ministry's compliance with the applicable requirements, despite the importance of these Regulations for protecting the privacy of individuals whose sensitive information is stored in the databases, and despite the significant risks these databases are exposed and their far-reaching implications for individuals, the organization, and national security.

- **Mapping and Registering the Databases of the Ministry of Defense** – Contrary to the requirements of the Privacy Protection Law, according to which a database controller will register these databases in the Database Public Registry and notify of certain changes relating to them, the Applications and Technology Department has not mapped all data controlled by the Ministry of Defense since 2007 to determine whether it contains personal data as defined in the Law and the Regulations, and whether

3 As reported in the media in April 2024 (for example, Israel Hayom, "Hackers Penetrated Ministry of Defense Systems: Concern That Sensitive Information Was Leaked" (April 9, 2024) https://www.israelhayom.co.il/tech/tech-news/article/15573329). The Ministry of Defense informed the media that a non-sensitive website had been breached, and confirmed this statement to the State Comptroller's Office in December 2024, as well as providing the investigation conducted following the incident and the measures taken to address the security breach.

4 As reported in 2022 in the media (for example, TheMarker, "A Small Excel Error Exposed Details of Senior Ministry of Defense Officials Online" (August 24, 2022) https://www.themarker.com/captain-internet/2022-08-24/ty-article/.premium/00000182-cf9f-d1de-a7c3-dfdf3bca0000). The Ministry of Defense confirmed the details to the State Comptroller's Office in September 2024.

additional legal requirements – such as registering such data in the Database Public Registry – apply to the Ministry.

As a result, the Ministry of Defense has not recognized that it may control additional databases for which it is required to act under the provisions of the Privacy Protection Law and the Regulations, including databases containing sensitive personal information such as data concerning a person's family life; medical information; criminal record; salary data; religious beliefs; ethnic origin; assessment of essential personality traits, including character, intellectual capacity, and work performance; their location and traffic data.

Sensitive personal information of this kind may be included, for example, in the Ministry of Defense's databases of reliability and security clearance evaluations conducted for all population sectors employed by the Ministry, as well as in its databases of professional evaluation tests for prospective employees. Accordingly, the Ministry is not aware that it may be subject to additional obligations regarding personal data controlled by it, as well as obligations under the Privacy Protection Regulations (Instructions for Data that was Transferred to Israel from the European Economic Area), 2023. Compliance with these obligations facilitates trade relations with the EU member states, and failure to comply may harm foreign relations with defense establishments that are very important for achieving the State of Israel's national security objectives.

Classification of Databases and Formulation of Means Intended to Protect Them – Contrary to the requirements of the Privacy Protection Regulations (Data Security), according to which a database definition document shall be prepared describing its key aspects and each database shall be classified according to the level of security risk it poses, the Applications and Technology Department of the Ministry of Defense has neither prepared such a document for each database under its control nor classified the databases according to the applicable security levels (medium or high). As a result, the Applications and Technology Department lacks a complete and up-to-date picture of all the databases it manages, that would enable it to formulate the means intended to Protect them according to the risks each database poses. Furthermore, beginning in August 2025, with the entry into force of Amendment No. 13 to the Privacy Protection Law, the Ministry of Defense is liable to be exposed to administrative financial fines ranging from NIS 20,000 to NIS 320,000 for various violations of the Data Security Regulations vis-à-vis each database.

Management of Access Authorizations in the Identity Management System[5]

- The audit found that, according to an analysis made by the State Comptroller's Office, 7 out of 10 external users with access permission to the Ministry of Defense's central computer network – which serves as a gateway to databases – had not

5 A computerized system in which user accounts are managed for roles with different access permission to the Ministry of Defense's computer networks, data systems and the databases linked to them.

logged into the network for more than six months; most of them (60%) had not logged in at all. This raises concerns that these users hold access permission that is not required for the performance of their duties. The audit further found that most of the users who had not logged into the network for more than six months (90%) were outsourced employees, and a large share of them (60%) were assigned to five departments, from which the potential risk of exposure of defense-related or personal data is high. Since this network serves as the gateway to databases, and contains assets – some of them are sensitive – as well as inputs that serve processes related to IDF business operations and procurement, the risk of personal data being exposed to unauthorized individuals is heightened.

- The audit further found that the Applications and Technology Department of the Ministry of Defense had not established a reporting mechanism for entities requiring authorization from the Ministry of Defense and IDF directorates to report the end of external users' service, in order to revoke their access authorizations. This is despite the fact that, due to the absence of a structured reporting mechanism, there are active but unnecessary access permissions within the external users group, including authorizations for computer networks and data systems that serve as gateways to databases.

- The audit also found that the Applications and Technology Department does not conduct a structured and systematic permission review on the thousands of users managed in the Identity Management System and the tens of thousands of authorizations' types it contains in order to update user lists. Instead, it occasionally performs targeted, manual examinations of access authorizations for a limited group of users, at its discretion. This does not comply with the Regulations' requirement to maintain an up-to-date record of users and the permissions granted to them for the performance of their duties, despite the Department being aware of unnecessary authorizations in the external users' group.

Management of Access Authorizations to the Disabled IDF Veterans Database

- The audit found that, according to an analysis made by the State Comptroller's Office, 5 out of 10 users with active access permission to the Shemesh system[6] (263 out of 481 users) had not logged into the system for more than six months. Of these, 29% (78 users) had not logged in at all. This raises concerns that they hold access permission without a functional need.

- The audit further found that the Ministry of Defense's Applications and Technology Department had not established a structured reporting mechanism for entities requiring authorization to report the end of external users' service in the Shemesh system, in order to revoke their access. This is despite the fact that, due to the absence of a structured reporting mechanism, there are external users who have

6 The Rehabilitation Department's central information system, which is linked to the Disabled IDF Veterans database.

active access permissions for Shemesh-system that are not required. For example, unnecessary active permission existed for workers employed via an external supplier, such as the Rehabilitation Department's call center which employs dozens of workers with high turnover, as well as for external contractors able to connect remotely to the Shemesh system, even after their service had ended.

As a result, under certain circumstances, unauthorized parties may be exposed to personal data, including particularly sensitive data, in the Ministry of Defense's Disabled IDF Veterans Database, which contains details on more than 230,000 individuals, including their health and economic status, family members, and the services provided to them. This risk is heightened by the addition of approximately 18,000 wounded individuals to the database due to the Swords of Iron War, and the resulting increase in the number of service providers in the Rehabilitation Department who use the Shemesh system. Once Amendment No. 13 to the Privacy Protection Law enters into force, the Privacy Protection Authority will be authorized to impose administrative financial fines on the Ministry of Defense for failing to revoke user access authorization immediately upon the end of their service, to the sum of NIS 160,000 for each high-security level database, such as the Disabled IDF Veterans Database.

- **Database Security Procedure** – The Applications and Technology Department has not established a database security procedure as required by the Regulations. Certain topics that must be included in such a procedure are addressed in procedures set by the Security Department, such as cyber security incident management, secure usage of portable devices and password policy, which forms part of the access policy for the databases. However, topics such as the risks to which the databases are exposed, the manners in which these risks are identified and dealt with, and the manners of monitoring the use of the databases are not addressed in procedures of any entity within the Ministry of Defense.

  In the absence of a database security procedure, the Ministry of Defense lacks a structured and comprehensive security policy for addressing the security risks to which the data in its databases is exposed, as well as a tool for conducting periodical audits to verify the existence of security measures required under such a procedure and their proper functioning.

- **Risk Assessment Surveys and Penetration Tests** – The Applications and Technology Department has not conducted risk assessment surveys to identify data security risks in the Ministry's high security level databases, nor has it performed penetration tests to the systems of these databases to assess their resilience against internal and external threats, as required by the Privacy Protection Regulations (Data Security). While the Applications and Technology Department and the Security Department do carry out risk assessment surveys and penetration tests for various Ministry of Defense networks, database systems, and Ministry of Defense websites

developed by external contractors, to detect potential vulnerabilities, no entity within the Ministry of Defense has conducted dedicated risk assessment surveys or penetration tests for the 14 databases controlled by the Ministry. The Ministry has not identified, analyzed or assessed possible scenarios for the occurrence of security incidents in these databases – whether individually or at stages of the business processes relating to them – nor estimated the likelihood of such scenarios materializing; it has not relied on a mapping of the characteristics of the database systems that process data from the databases, or included a mapping of the existing controls in the organization against those that should be implemented to minimize the likelihood of the risks materializing. As a result, the Ministry has not examined the need to update the database definitions document or the database security procedure, has not determined the necessary controls, and has not assessed the effectiveness of the existing controls and protection mechanisms.

In the absence of risk assessment surveys and penetration tests for its databases, the Ministry of Defense lacks the tools to assess its maturity level in addressing threats to the integrity, confidentiality, and availability of the data stored in the databases; to identify weaknesses in data security; to prioritize the handling of these risks; to understand the controls it must implement in its work plans; and to evaluate the effectiveness of the controls and the existing defense mechanisms.

Appointment of a Data Security Officer for the Ministry of Defense's Databases – Following this audit, in October 2024 the Head of the Applications and Technology Department appointed a new Data Security Officer for the Ministry of Defense's databases and granted her powers and responsibilities in line with the Data Security Regulations. Until then, the Head of the Applications and Technology Department had not ensured that the Ministry's Data Security Officer was fulfilling her duties as required.

Database Mapping – Following the audit, in December 2024, the Head of the Applications and Technology Department instructed the heads of the Ministry of Defense's departments and units to map the databases within their respective departments and units. It should be noted that his directive applied only to data transferred from the Ministry of Defense to external entities or received from them. As of the end of the audit, in January 2025, the mapping had not yet been completed.

Key Recommendations

- The Ministry of Defense should comply with the privacy protection requirements applicable to it under the Law and the Regulations, particularly in light of Amendment No. 13 to the Law, which will enter into force in August 2025 and align the legislation with contemporary challenges. In addition, given the findings from the State Comptroller's data analysis, it is recommended that the Ministry review its authorization management processes across all database systems connected to its databases. It is further recommended that the Director General of the Ministry of Defense regulate the division of responsibilities and authorities between the Applications and Technology Department and the Security Department in the field of database data security from the privacy protection perspective. This will help reduce the risks of privacy violations and of impairing the Ministry of Defense's ability to fulfill its mission.

- The Head of the Applications and Technology Department – tasked with managing the Ministry of Defense's databases – should ensure that the Data Security Officer for these databases is capable of fulfilling her role as required, that she receives the necessary training, and that the necessary resources are allocated to the task. The Data Security Officer for the Ministry of Defense's databases should carry out her role as stipulated in the Regulations, including preparing a plan for ongoing monitoring in regard to compliance with the Regulations' requirements, implementing this plan and notifying all relevant stakeholders of the findings. The Director General of the Ministry of Defense should appoint a Privacy Supervisor, as mandated by Amendment No. 13 to the Privacy Protection Law coming into force in August 2025, ensure that there is a clear division of responsibilities between the Data Security Officer for the Ministry's databases and the appointed Privacy Supervisor, and monitor the execution of their respective roles.

- The Head of the Applications and Technology Department should instruct the heads of the departments and units in the Ministry of Defense to carry out a comprehensive mapping of all personal data in their possession, not only of the data transferred from the Ministry of Defense to external entities or received from them. He should also ensure that the mapping addresses the Privacy Protection Regulations (Instructions for Data that was Transferred to Israel from the European Economic Area), 2023. Following this, the Head of the Applications and Technology Department should identify the requirements applicable to the Ministry of Defense based on the mapping's findings, including the obligation to register such databases in the Database Public Registry.

- The Applications and Technology Department should periodically review all existing authorizations in the database systems connected to the Ministry of Defense's databases, including the Shemesh system, which is connected to the Disabled IDF Veterans Database, and revoke active authorizations that are not necessary for users to perform their duties. In addition, it is recommended that the Department also examine the

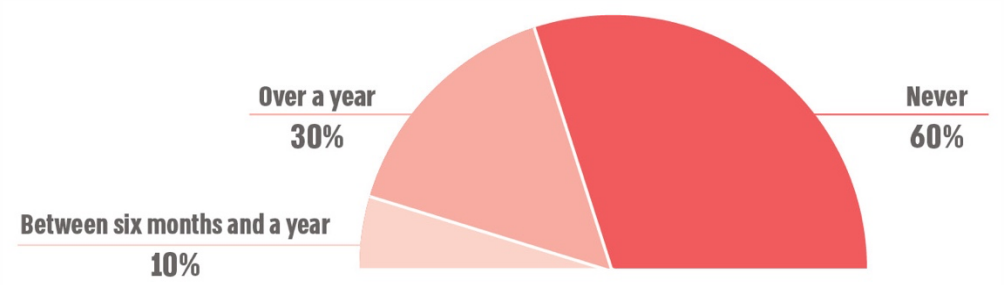
authorization management processes in the database systems. This will help reduce the risk of exposing personal data, including particularly sensitive information, to unauthorized individuals, as well as the risk that such data will be leaked, rendered unavailable or tampered with. In this way, the risk of harm to the privacy of individuals whose personal data is stored in the databases will be reduced.

It is recommended that the Director General of the Ministry of Defense will regulate the division of responsibilities and authorities regarding data security under the Privacy Protection Law and the Data Security Regulations. This may be done, for example, by appointing a single entity with overall responsibility and a comprehensive view of all aspects of data security, including privacy protection considerations; by establishing an inter-department team to strengthen data security, comprising, for example, representatives from the Security Department, the Applications and Technology Department, the Office of the Legal Advisor to the Defense Establishment, and departments that use the databases; or by any other means deemed appropriate. It is further recommended that the division of responsibilities, authorities, and various roles, including with reference to Amendment No. 13 to the Privacy Protection Law, be anchored in a ministry procedure.

The Potential Risk of External Users with Unnecessary Access Authorizations to a Central Computer Network of the Ministry of Defense

The Percentage of External Users who have not Logged in to the Network for more than Six Months of all External Users with Active Network Access Permission

Distribution of the Last Login Date of External Users who have not Logged in to the Network for more than Six Months



According to data from the Applications and Technology Department, processed by the State Comptroller's Office.

Given that this network serves as the gateway to the Ministry's databases, hosts assets – some of them sensitive – and supports the IDF's business operations and procurement processes, the risk of exposing sensitive information to unauthorized parties is increased, especially since 90% of the external users who have not logged in to the network for more than six months are outsourced workers.

Summary

The Ministry of Defense controls databases containing personal data, such as data on a person's personality traits, health condition, and financial status. The risks to privacy and data security in these databases have increased, in light of the Swords of Iron War, and their materialization could impair the Ministry's ability to provide the Israel Defense Forces with the required resources, could cause reputational damage, harm relations with suppliers and customers, and expose it to fines. Moreover, such risks could sow panic and a sense of insecurity among the public, and damage the state's foreign relations in security and diplomatic contexts.

In recent years, data has leaked from the Ministry of Defense – both as a result of cyberattacks by hostile external actors and due to human error on the part of Ministry employees, including identifiable data about Ministry of Defense personnel.

The situation described in this report indicates serious gaps in the way the Ministry of Defense manages and secures the 14 databases under its control, which contain personal data on 2.84 million individuals. The audit found that the Applications and Technology Department, which is responsible for ensuring that the Ministry of Defense complies with the requirements imposed under the Privacy Protection Law and the Privacy Protection Regulations (Data Security), has not mapped all the databases controlled by the Ministry of Defense since 2007; has not established a data security procedure for the databases; has not conducted risk assessment surveys to identify data security risks in the databases that are classified as high security level; and has not performed penetration tests to the systems of these databases to assess their resilience against internal and external threats.

In addition, the report identified shortcomings in the management of user authorizations in the identity management system and in the database system linked to the IDF Disabled Veterans Database – a database containing data on approximately 230,000 individuals, including approximately 18,000 wounded persons added to the data as a result of the Swords of Iron War, with details on their health condition, financial status, family members, and the services provided to them. An analysis conducted by the State Comptroller's Office found that 5 out of 10 external users (outsourced employees) with active access permission to the database system linked to the IDF Disabled Veterans Database had not logged into it for more than six months. Furthermore, consultants managed in the Ministry of Defense's human resources systems, in the same way as ministry employees, had also not accessed the system for more than six months; their share of all users who had not logged in during that period was 20%. This situation raises concerns that they hold access authorizations to the IDF Disabled Veterans Database without necessity.

The Ministry of Defense should comply with the privacy protection requirements applicable to it under the Law and Regulations, particularly in light of Amendment No. 13 to the Law, which will enter into force in August 2025 and adapt the Law to current challenges. In addition, given the findings from the data analysis conducted by the State Comptroller's Office, it is

recommended that the Ministry examine its authorization management processes across all database systems connected to the Ministry's databases. It is further recommended that the Director General of the Ministry of Defense regulate the division of responsibilities and authorities between the Applications and Technology Department and the Security Department regarding data security from a privacy protection perspective. This will help to reduce the risks of privacy violations and of impairing the Ministry of Defense's ability to fulfill its mission.

Report of the State Comptroller of Israel |
December 2025

Ministry of Defense

Employment of Consultants in the Ministry of Defense

Employment of Consultants in the Ministry of Defense

Background

The main activities of the Ministry of Defense are carried out by civil servants employed by the Ministry. However, in many cases, due to the need for a person with special knowledge or expertise to carry out certain tasks for a limited period of time, the Ministry engages with companies that provide consultants or with independent consultants. The Ministry of Defense employs external consultants and external personnel (consultants) in various fields and projects, for different periods and at varying levels of employment.

The Consultants and External Personnel Unit in the Planning Department of the Ministry of Defense (the Consultants Unit) is responsible for reviewing and approving the engagement of consultants for the Ministry. The Ministry of Defense directive on the employment of consultants and external personnel sets rules limiting the scope of consultant employment in terms of the average monthly working hours and the number of years a consultant may be employed by the Ministry (employment tenure).

.

Key Figures

1,235

The number of consultants employed by the Ministry of Defense on a full-time equivalent (FTE) basis as of October 2024. In total, 2,509 consultants were engaged at varying levels of employment

vs. 2,490

The maximum workforce amount of regular (permanent) employees allowed by the Ministry in 2024

1:2 one external consultant for every two Ministry of Defense employees

The ratio of full-time-equivalent consultants (1,235) to regular employees (2,490) as of October 2024

NIS 510 million

Total sum of orders for consultants in 2024 compared with the Ministry's 2024 salary budget for regular personnel, which amounted to NIS 1.2 billion

685 (27%)

The number (and proportion) of consultants whose scope of employment as of October 2024 exceeded the Ministry of Defense's rules regarding average monthly working hours and employment tenure

315 (46%)

The number (and proportion) of consultants, out of the 685, whose scope of employment significantly exceeded the Ministry of Defense's rules as of October 2024, i.e. more than ten years of employment or more than 180 average monthly working hours

Only 3 women

The number of female consultants among the 20 consultants with the highest paid contracts as of October 2024

320 (13%)

The number (and proportion) of consultants employed by the Ministry of Defense as of October 2024 under more than one contract, for whom no method was defined for calculating average monthly working hours for the purpose of checking compliance with the working-hours limit

Audit Actions

In the months of August 2024 to January 2025, the State Comptroller's Office examined the following aspects of consultants employment in the Ministry of Defense: the strategy for employing consultants; the overarching view of the Ministry's human resources; the scope and duration of consultant employment; and oversight processes in the employment of consultants. The audit was conducted in the Ministry of Defense's Planning Department; Defense Establishment Legal Advisor; Finance Department; Human Resources Department; Engineering and Construction Department; International Defense Cooperation (SIBAT); Application and Technology Department; and IDF Southern Relocation Administration.

Key Findings

Scope of Consultant Employment in Ministry of Defense Units – Consultants are employed in all departments and units of the Ministry of Defense. Consultants are intended to be engaged for a limited period to perform specific tasks, inter alia to ensure fair competition and to reduce the Ministry's dependence on any individual consultant. For this reason, the Ministry of Defense sets rules, in its directives, limiting a consultant's working hours based on the length of their employment with the Ministry. As of October 2024, the scope of employment of 685 of all consultants engaged by the Ministry (27%) exceeds these established limits. Of these 685 consultants, 315 (46%) are employed in breach of the maximum working hours and/or maximum tenure – i.e., more than ten years of employment or more than an average of 180 monthly working hours, or both. Approximately half of these consultants (153) were employed in the Engineering and Construction Department, the Application and Technology Department, the IDF Southern Relocation Administration, and the International Defense Cooperation (SIBAT). In doing so, the Ministry of Defense fails to comply with the limits on consultant employment it set for itself, thereby harming fair competition and equal opportunities, increasing its dependence on consultants, raising the risk of establishing employer–employee relationships with them, raising the risk of creating a parallel track for employing personnel outside the regular staffing framework, and increasing the risk of loss of organizational knowledge, particularly when engagements continue for many years.

Formulation and Dissemination of a Strategy for Employing Consultants in the Ministry of Defense – The Ministry of Defense has not formulated a strategic document on the employment of consultants. Consequently, the Ministry has no written strategy consolidating all objectives, targets, and courses of action on consultant

employment, including organization-wide guiding principles such as the prohibition on employing consultants in managerial positions or in positions involving the granting of authorizations. This is despite the employment of 1,235 consultants (in full-time equivalent terms) at a financial scope of NIS 510 million, representing 30% of the total expenditure on consultants and regular personnel combined1. The Deputy Director-General and Head of the Human Resources Department stated that the Human Resources Department is not aware of whether the Ministry of Defense has a strategy for managing consultants; and the Senior Deputy to the Head of the International Defense Cooperation (SIBAT) stated that the Defense Exports Directorate is not familiar with any Ministry strategic document setting out organization-wide guiding principles. In practice, the Ministry's officials lack an official document on which they can base their work or against which they can be assessed, a situation that may lead to differing interpretations among the departments regarding consultant employment policy. Accordingly, in the absence of a strategic document on the employment of consultants, it cannot be ensured that the Ministry's managers are aware of, and act in accordance with, the objectives, targets, and courses of action that the strategy is intended to set out.

- **Overarching View of Human Resources in the Ministry of Defense –** The management of human resources in the Ministry of Defense, including the planning and monitoring of an optimal mix of regular employees and consultants, does not reflect a complete, organization-wide strategic perspective. When the Organization Unit responsible for regular employees and the Consultants Unit responsible for consultants operate separately, each focuses on a different part of the overall human resources picture in the Ministry – 2,490 regular employees and 1,235 consultants (in full-time equivalent terms) as of October 2024, i.e., one full-time consultant for every two regular employees – and there is no integrated view of the Ministry's total human resources, 3,725 employees and consultants in that year. This situation compromises the Ministry's planning and oversight with respect to the optimal mix of regular employees and consultants.

- **Gender Equality in the Employment of Consultants –** Under section 2B(b) of the Mandatory Tenders Law (section title: Encouragement of Women in Business), when two or more bids receive an identical weighted score that is also the highest score, the bid of a business controlled by a woman is to be selected. This reflects a legislative policy of preference for women. However, it was found that only 15% of the 20 consultants whose contractual budget scope with the Ministry of Defense was the highest as of October 2024 were women (just 3 women out of 20). It should be noted that the average monthly contractual scope for each of these 20 consultants was NIS 65,000.

- **Consultants with More Than One Contractual Agreement –** In the case of a consultant with multiple contractual agreements (320 of all consultants as of October

1 The data are correct as of 2024.

2024 (13%)), the Ministry of Defense's directive on the employment of consultants does not set out how to calculate the average monthly number of hours for the purpose of checking compliance with the limit on average working hours. It was found that, according to the State Comptroller's Office calculation, of the 320 consultants employed by the Ministry of Defense under more than one contractual agreement, 36 (11%) were employed for more than 180 monthly hours as of October 2024. The total value of the contracts for these consultants amounted to approximately NIS 19.5 million. In the absence of a definition in the directive, the Consultants Employment Unit does not examine the scope of consultant employment in the Ministry of Defense according to orderly and equal criteria. This may result in consultant employment in the Ministry of Defense that contravenes the rules set in the directive.

- **Oversight Processes in the Employment of Consultants –** The Planning Department in the Ministry of Defense does not carry out comprehensive and orderly oversight processes regarding the employment of consultants, which constitute a key resource for the Ministry (in 2024, orders for consultants totaled NIS 510 million, representing 30% of total expenditure on both consultants and regular personnel combined). The Planning Department has not formulated detailed metrics for monitoring actual performance against planned targets in aspects such as the number of consultants employed, the number of consultants in full-time equivalent terms, and scopes of employment in breach of the rules; there is no monitoring of consultant employment in breach of the rules; the current information system cannot generate reports in various breakdowns and at different levels, such as reports on scopes of employment in breach of the rules; and periodic oversight discussions providing a broad overview of the subject are not held by the Deputy Director-General and Head of the Planning Department. Accordingly, there is no orderly reporting and oversight mechanism that could provide a situational picture regarding consultant employment, thus enabling those with responsibility and authority to make decisions and give appropriate instructions to achieve objectives and comply with the Ministry's directives.

- **Recording of Rejected Requests to Employ Consultants –** The Consultants Unit does not maintain in its information systems a record of requests from the Ministry of Defense's departments and units to employ consultants that have been rejected. As a result, the Ministry of Defense cannot perform computerized monitoring of all requests, including those rejected by the Committee for the Employment of Consultants and External Personnel, and therefore has neither a complete picture of this matter within the Ministry nor the ability to draw lessons in order to improve recruitment and selection processes for consultants.

- **Evaluation of Consultant Performance –** (a) The Ministry of Defense does not conduct a structured, organization-wide process for evaluating the performance of its consultants (apart from certain ad hoc processes in specific departments). In addition, the Planning Department in the Ministry of Defense does not instruct all of its departments to carry out performance evaluations for the consultants they employ. As a result, the Ministry lacks both a comprehensive and detailed picture of the quality of its

consultants, and it is possible that the Ministry continues to employ consultants whose performance is below standard. (b) Although some of the Ministry's departments do carry out internal performance evaluations of their consultants, the evaluation results are not shared with other departments. This is contrary to the Ministry of Defense directive on supplier performance evaluation. As a result, any department wishing to employ a consultant previously engaged by another department has no access to that department's performance evaluation. This deprives it of important information needed when deciding whether to hire the consultant. Such a situation may lead to the hiring of a consultant who has previously provided deficient service and received a low performance evaluation in another department.

Key Recommendations

- It is recommended that the Deputy Director-General and Head of the Planning Department formulate a strategic document on the employment of consultants in the Ministry of Defense, submit it for the approval of the Director-General, and disseminate it to all managers in the Ministry. The purpose of this is to ensure that the Ministry's entire management echelon is aware of its strategy for employing consultants; to ensure a uniform interpretation of the objectives, targets, and courses of action outlined by the Ministry; and to ensure transparency with the management and the ability to monitor processes and the achievement of objectives. The document may stand alone or be incorporated into the Ministry's overall organizational staffing strategy, provided that it maintains a clear distinction between the employment of permanent Ministry employees and employment through engagement with consultants – with all that this entails, including the types of tasks and areas of responsibility assigned to them.

- It is recommended that the Ministry of Defense take steps to increase the number of female consultants it employs. For example, the Ministry can raise awareness among the departments and its units that employ consultants regarding the importance of employing women. It is further recommended that, as part of formulating a strategic document on the employment of consultants, the Ministry of Defense set measurable objectives and targets in the area of gender diversity.

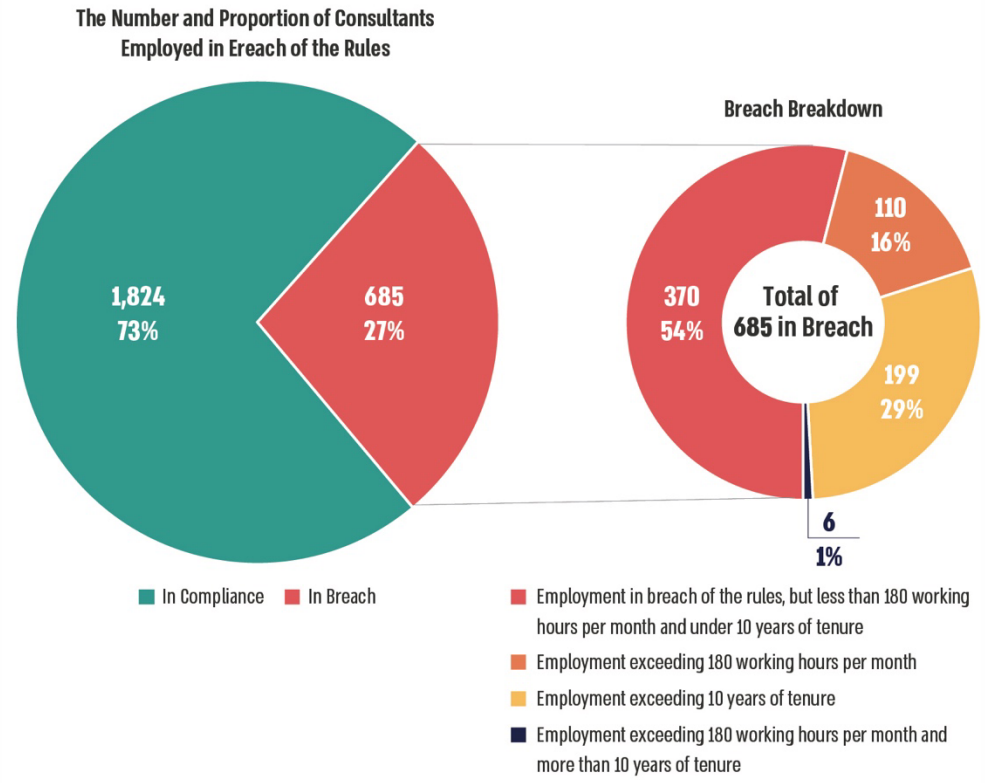
- It is recommended that the Deputy Director-General and Head of the Planning Department review work processes and implement organizational adjustments that will enable a wide organization strategic perspective on the Ministry of Defense's human resource needs. For example, this could include involving the Organization Unit in the process of examining personnel substitution that is carried out by the Consultants Unit. This would allow for more efficient management of the Ministry's human resources, a comprehensive and in-depth approach to the Ministry's needs, and the tailoring of solutions to those needs.

- In view of the extensive employment of consultants – some of them in key positions – who are engaged in breach of the rules set in the Ministry of Defense directive on the employment of consultants, it is recommended that the Planning Department in the Ministry of Defense, together with the Defense Establishment Legal Advisor, re-examine the rules set in the directive regarding the scope of consultant employment and their tenure. This should include criteria for approving deviations from the rules, and the formulation of an updated approach to the restrictions imposed by the rules and the objectives they are intended to serve – including reducing the Ministry's dependence on consultants, decreasing the risk of creating employer–employee relationships, ensuring fair competition and equal opportunities, and preserving organizational knowledge.

- It is recommended that the Planning Department in the Ministry of Defense carry out comprehensive and orderly oversight processes regarding the employment of consultants, establish clear metrics for ongoing monitoring, and conduct oversight of consultant employment in breach of the rules. Possible examples of such metrics include: the number of consultants under contract; the number of consultants in full-time equivalent terms; the ratio of regular employees to consultants; and the scope of deviations from the rules on consultant employment in terms of monthly hours and duration of employment. It is further recommended that the Planning Department ensure that the process for upgrading the information system in the Consultants Unit is implemented and supports effective oversight processes regarding consultant employment. In addition, it is recommended that the Deputy Director-General and Head of the Planning Department hold periodic oversight discussions on consultant employment in the Ministry of Defense and present an annual status report to the Director-General of the Ministry of Defense.

- It is recommended that the Planning Department instruct all of the Ministry of Defense's departments to carry out performance evaluations for the consultants they employ, and establish and operate an organization-wide mechanism for evaluating consultant performance that will provide both a comprehensive and detailed picture of the area of consultant activity in the Ministry.

Breakdown of the Scope and Proportion of Consultant Employment in the Ministry of Defense in Breach of the Rules (October 2024)



According to Ministry of Defense data, processed by the State Comptroller's Office.

Summary

The Ministry of Defense has numerous tasks and carries out many projects, some of them national in scope, and therefore requires the services of consultants with special knowledge, expertise, or skills. As of October 2024, the Ministry employed 2,509 consultants at varying levels of employment, equivalent to 1,235 full-time consultants, compared with 2,490 regular employees (a ratio of 1:2). In that year, orders for consultants totaled NIS 510 million, and the salary budget for regular personnel was approximately NIS 1.2 billion.

Consultants are intended to be engaged for a limited period to perform specific tasks, in a manner designed to ensure fair competition and to reduce the Ministry of Defense's dependence on them. Accordingly, the Ministry of Defense set in its directive rules limiting consultants' working hours according to the duration of their employment with the Ministry.

The audit found that, as of October 2024, the scope of employment of 685 consultants out of all consultants engaged by the Ministry of Defense (27%) exceeded the limits set in the Ministry's directive on the employment of consultants. The audit further found that the Planning Department in the Ministry of Defense does not carry out comprehensive and orderly oversight processes regarding the employment of consultants; that the Ministry of Defense does not conduct a structured and systemic process for evaluating consultant performance; and that the Ministry has not formulated a strategic document on the employment of consultants consolidating all objectives, targets, and courses of action on the subject.

The Director-General of the Ministry of Defense should act to rectify the deficiencies raised in this report regarding the employment of consultants, particularly in view of the significant scope of such employment and its implications. It is also recommended that the Deputy Director-General and Head of the Planning Department in the Ministry of Defense formulate a strategic document on the employment of consultants in the Ministry, review work processes, and implement organizational adjustments that will enable a systemic strategic perspective on the Ministry's human resource needs. It is further recommended that the Deputy Director-General and Head of the Planning Department carry out comprehensive and structured oversight processes regarding consultant employment, and re-examine the rules set in the Ministry of Defense directive regarding the scope of consultant employment and their tenure, while formulating an updated approach to the restrictions imposed by the rules. In addition, it is recommended that the Ministry of Defense establish and operate a mechanism for evaluating consultant performance.

Report of the State Comptroller of Israel |
December 2025

Ministery of Defence

Aspects of the Ministry of Defense's Supervision and Control of Defense Companies' Use of Marketing Promoters, Agents, and Brokers in Defense Export

Aspects of the Ministry of Defense's Supervision and Control of Defense Companies' Use of Marketing Promoters, Agents, and Brokers in Defense Export Transactions

Background

As part of the international marketing of their products, the defense companies make use of external entities working on their behalf to promote transactions between them and third parties in return for a commission, wage, or other compensation[1] (marketing promoters, agents, brokers).[2]

The Defense Export Control Law, 2007 (the Export Control Law) and the regulations enacted under it aim to regulate the state's supervision of defense exports[3] for reasons of national security, foreign relations, and international commitments and to protect other critical national interests. The law stipulates that no Israeli citizen, resident, or corporation may engage in defense marketing – acting with the goal of promoting defense exports, including brokering a defense export transaction[4] – unless they have received a license to do so from the competent authority[5] (marketing license).

In 2005, Israel signed the UN Convention Against Corruption (UNCAC) and ratified it in a government decision in December 2008.[6] In 2009, Israel ratified the OECD[7] Convention on Combating Bribery of Foreign Public Officials in International Business Transactions[8],[9] (the OECD Convention), and it is obligated to implement their directives. Within the framework of Israel

1 The company's agreement with the marketing promoter sometimes includes payment contingent on success as the exclusive payment, in addition to the regular payment, or as an additional payment to cover costs.

2 The defense companies and the Ministry of Defense use one or more of these terms.

3 Exports of military equipment, transfer of military knowledge, or provision of security service.

4 Performed in Israel or abroad, in writing, orally, or in any other manner, directly or indirectly, for consideration or not, whether or not the action involves the transfer of security knowledge, or conducting negotiations for the promotion of such a transaction. The Export Control Law also stipulates that it makes no difference whether or not the defense export transaction has been carried out.

5 According to the law, the competent authority is the Director General of the Ministry of Defense, the Head of the Defense Export Controls Agency (DECA), or a senior employee at DECA that the Director General has authorized for the purposes of the Export Control Law.

6 On December 22, 2008, the government of Israel decided to ratify the convention (decision no. 4355).

7 Organisation for Economic Co-operation and Development

8 On February 12, 2009, the government of Israel decided to ratify the convention (decision no. 4481).

9 OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions.

joining the OECD, the Ministry of Defense (MOD), through the Ministry of Justice, committed to implementing mechanisms to prevent the offense of bribing a foreign public servant.

In July 2008, in anticipation of Israel joining the UN Convention, an offense was added to the Penal Law, 1977, regarding bribing a public servant of a foreign country or an employee of an international public organization. According to the law, it is prohibited to offer or provide a bribe to a foreign public servant in order to attain, ensure, or promote business activity, or to attain an advantage related to such activity.

Implementation of the OECD Convention is supervised by the OECD Working Group on Bribery in International Business Transactions[10], of which Israel is a member. The Working Group prepared a document including a series of recommendations, and in November 2021, the OECD adopted these recommendations for the organization.[11] Among other things, the document recommends that countries encourage companies and business organizations to develop ethics and compliance measures or programs to detect or prevent bribery of foreign public servants, including through third parties, such as agents.

The purpose of using marketing promoters in defense export transactions is to promote sales and increase the likelihood that a business opportunity will develop into a transaction. However, their use involves considerable compliance and regulatory risks, given the provisions of the Penal Law and the OECD conventions. If marketing promoters of defense export transactions perform actions that violate Israeli and international law – that is, provide a bribe to foreign public servants – this could lead to a range of legal consequences for the corporation and the people involved, undermining the reputation and standing of the company, Israel's international standing, and its ability to continue to carry out defense export transactions if it is blacklisted.[12] This risk is exacerbated by the intense competition that exists in the international defense market and in view of defense export and marketing activities that also take place in countries with high levels of corruption, where the expectation of receiving bribes for defense export transactions can be higher.

Another risk inherent in the use of marketing promoters relates to the employment of marketing promoters who have personal connections with senior MOD officials, who can influence the decision-making process on defense exports. The concern is that these connections will lead to conflicts of interest and consequently to undue benefits and sub-optimal decision-making in the MOD regarding such transactions, and will violate the right to equal opportunity. The materialization of this risk could also undermine public confidence in public administration.

From 2018 to 2023, Israel's defense exports totaled $60.5 billion.

10 OECD Working Group on Bribery in International Business Transactions.

11 Update of directives from November 2009.

12 On blacklists that include information on companies and other entities suspected or accused of violating international trade laws, regulations, or norms, and trade restrictions are imposed on them.

Key Figures

16 years ago

The offense of providing a bribe to a public servant of a foreign country or to an employee of an international public organization was added to the Penal Law, with a maximum penalty of seven years in prison[13]

64

The State of Israel's grade in 2024 in the Corruption Perceptions Index, on a scale of 0 (high level of corruption) to 100 (a corruption-free country). Israel ranked 30th out of 180 countries

$13.1 billion

Israel's total defense exports in 2023

Hundreds of millions of dollars

Total amount that defense companies committed to paying marketing promoters for transactions from 2022 to 2024

A significant proportion

of the defense export transactions made from 2022 to 2024, worth billions of dollars, involved marketing promoters

Audit Actions

From August to December 2024, the Office of the State Comptroller examined aspects of the MOD's monitoring of defense companies' use of marketing promoters in defense export transactions, including the MOD's policy on this issue; the interface between the defense companies and the MOD with respect to the activity of marketing promoters, including its monitoring of the issue; and the regulation of the MOD's activity in contexts related to this issue in its directives and procedures. Supplementary examinations were conducted until February 2025. The audit was conducted within the MOD, at the Office of the Director General of the MOD, the Department of the Defense Establishment Legal Advisor, SIBAT-International Defense Cooperation, the Directorate of Defense Research & Development, the Defense Export Controls Agency (DECA), the Policy & Political-Military Bureau, and the Planning Department. A supplementary audit was conducted at

13 Or a fine, according to the higher of the following: 1. In an amount of up to approx. NIS 1.1 million against an individual or approx. NIS 2.2 million against a corporation. 2. Four times the value of the benefit that was calculated or that there was an intention to attain by means of the offense.

the Ministry of Justice. The audit did not address suspicions of violations of the law or prosecution for offenses involving bribing foreign public servants.

The subcommittee of the Knesset's State Control Committee decided not to table place this report in its entirety on to the Knesset's table, but and only to publish only parts of it, in order to maintain national security, in accordance with Article 17 of the State Comptroller Law, 1958 [consolidated version].

Key Findings

The MOD's Involvement in Defense Companies' Use of Marketing Promoters

- Despite the MOD Director General's November 2017 directive, there are no documents at the Department of the Defense Establishment Legal Advisor and the Office of the Director General indicating that they have considered the establishment of a mechanism to conduct periodic audits to check the defense companies' compliance with the rules, and no such mechanism has in fact been established.
- No administrative work documents on marketing promoters presented for the Director General's approval were found at the Office of the Director General and at SIBAT, and such administrative work is unknown to current position-holders at the MOD. The lack of documentation of administrative work performed under the instruction of the MOD's Director General undermines tracking and supervision of this issue. In addition, the Office of the Director General and the Planning Department do not have documentation that they have considered using the Defense Establishment Auditor's Unit to examine work processes at defense companies regarding the use of marketing promoters. The lack of documentation raises doubts about the performance of effective tracking of the implementation of the Director General's directives.
- During the advancement of a certain transaction that began to take shape in 2020, personnel at the MOD were by chance exposed to the marketing promoter involved in the transaction and to the high fee he was supposed to be paid, and they prevented its implementation under these conditions. This incident highlights the need for the MOD to determine how it must supervise defense companies' use of marketing promoters in defense export transactions, including with respect to the identity of the marketing promoters; the fees they receive, in general and in relation to the scope of their work; and the way fees are approved by the relevant defense company.

- Despite the understanding of MOD directors general since at least July 2022 regarding the need to formulate a position on the ministry's involvement in supervision of defense companies' use of marketing promoters in defense export transactions, and despite their recurring directives since July 2022 that the Deputy Director General and Head of the Planning Department and the Defense Establishment Legal Advisor should set rules regarding supervision of the use of marketing promoters, the MOD had not formulated a position on this issue as of the audit completion date in February 2025. Since the Director General has not determined the appropriate level of the ministry's supervision of marketing promoters in defense export transactions, the MOD is not maintaining proper oversight of this issue or optimally managing the compliance risks inherent in it .

- Despite decisions by MOD directors general in November 2017 and October 2020 that the MOD will require a statement from defense companies that the transaction, including the fee paid to the marketing promoter, has been approved by the company's board of directors, as a general rule, the MOD does not require this statement from the companies.

The MOD's Supervision of Defense Companies' Compliance with OECD Guidelines to Prevent Bribery and Corruption

- **Compliance Program to Prevent Corruption –** Although in 2017 it was reported to the OECD Working Group on Bribery in International Business Transactions that letters from the MOD's Director General on this matter are distributed annually to all defense exporters – after the distribution of the letters in 2015, 2016, and 2017, additional letters from the MOD's Director General were only distributed in 2020 and during the audit (September 2024).

- **Requirement to Implement Compliance Measures to Prevent Corruption within Small and Medium-sized Defense Companies –** From 2018 to 2023, small and medium-sized defense companies signed defense export contracts totaling billions of dollars. During those years, these companies signed many defense export contracts. It is important to note that in 2023, dozens of small and medium-sized companies signed defense export contracts.

  Since 2011, the MOD has required large defense companies to implement compliance programs to prevent corruption, and it later encouraged the rest of the defense companies to adopt such programs. Small and medium-sized companies sign many defense export transactions each year; these transactions entail compliance and regulatory risks regarding bribery and corruption. However, the MOD's Director General and the Head of DECA have not determined which measures small and medium-sized defense companies should adopt to prevent corruption in defense export transactions – an issue on which they have not yet formulated a position. Without defining these measures, there is no certainty that small and

medium-sized companies will take sufficient action to reduce bribery and corruption risks in their export transactions.

- **Supervision of Compliance Programs to Prevent Corruption –** Despite the role of the MOD Director General and the Head of DECA as supervisors of defense exports in accordance with the Export Control Law, no decision has been formulated at the MOD regarding supervision of the compliance programs of defense companies or of their nature and scope. In the current situation, the MOD's level of supervision is low. Without a decision, there is no certainty that the MOD's supervision of the implementation of the OECD's recommendations on bribery is optimal.

- **Statement within the Framework of Agreements Related to Defense Exports –** The MOD does not require defense company exporters to provide information on marketing promoters in export transactions.

- **Submission of Individual Statement to the Defense Establishment Legal Advisor –** The MOD lacks rules clarifying the circumstances in which companies must request and receive individual statements regarding marketing promoters from the Legal Advisor or the exporting company's compliance officer.

- **Information on Marketing Promoters –** Deficiencies were revealed in the MOD's supervision of this issue.

Involvement of the Boards of Directors of Defense Companies in Approving Engagements with Marketing Promoters, Including the Fees Paid to Them – The rules determined by boards of directors on this matter must be improved.

Normative Regulation of Marketing Promoters in the MOD

- **Regulating the MOD's Activity to Ensure Defense Companies' Compliance with the OECD Guidelines –** The MOD's directives do not include a directive that regulates the activities that the relevant MOD departments must take to implement the supervision of defense exports with respect to preventing bribery and corruption, including in the directive on the supervision of defense exports. Without regulation of this issue, there is concern that the necessary actions will not be properly taken and that the MOD's supervision, including with respect to the State of Israel's commitments under the OECD Convention, will be insufficient.

- **Regulation of Conflicts of Interest in the Activities of Marketing Promoters in Defense Export Transactions –** The marketing promoters are relevant businesspeople, or people who have previously served in senior defense positions in Israel or abroad, or people who know the decision-makers in the destination country. The MOD does not monitor the identity of the marketing promoters, and thus exposes itself to risk with respect to Israeli marketing promoters whose familiarity with senior figures in the MOD could lead to conflicts

of interest and consequently to undue benefits, sub-optimal decision-making in the MOD regarding these transactions, and violating the right to equal opportunity. The materialization of this risk could also undermine public trust in public administration.

Unlike the directive on the involvement of agents active in procurement transactions at the MOD, the MOD lacks a directive regulating the interactions of MOD employees with marketing promoters in defense export transactions, including with respect to conflicts of interest. The lack of regulation of this issue could lead to biases in decision-making processes regarding defense export transactions, including concerns about exploiting connections to advance personal interests that are not aligned with the MOD's interests.

- **Regulation of Fees Paid to Marketing Promoters in Defense Export Transactions –** Since the MOD's directive on Fees in Export transactions was changed in 2014, the MOD has not properly supervised defense companies' use of marketing promoters, including the fees paid to them.

  Following the cancellation of the directive on Fees in Export transactions in 2018, no alternative directive was formulated at the MOD on fees paid to marketing promoters in transactions involving defense companies, even after MOD directors general noted the need to regulate this issue.

- **Regulating the Interface Between MOD Employees and Marketing Promoters of Defense Companies –** The MOD lacks a directive governing interactions with marketing promoters. Without such regulation, there is a risk that MOD personnel will interact with marketing promoters in ways that expose the ministry to increased compliance risks.

Key Recommendations

The MOD's Involvement in Defense Companies' Use of Marketing Promoters – The Director General of the MOD should ensure that the Head of the Planning Department and the Defense Establishment Legal Advisor act promptly to formulate recommendations regarding the ministry's level of involvement in supervision of defense companies' use of marketing promoters, including the issue of fees. It is recommended that this be done in consultation with the Ministry of Justice's Legal Counsel and Legislative Affairs Department. This need is even more urgent given the significant increase in the volume of transactions in recent years, which is expected to expand further in the coming years.

The MOD's Supervision of Defense Companies' Compliance with OECD Guidelines to Prevent Bribery and Corruption

- **Requirement to Adopt and Implement a Compliance Program to Prevent Corruption –** It is recommended that the Director General of the MOD instruct the ministry to examine and submit a recommendation for his approval on minimum compliance rules that small and medium-sized companies should adopt and implement to reduce bribery and corruption risks in defense export transactions, including regarding due diligence on marketing promoters, especially given the large number of transactions that these companies sign each year, the risk of violations of the compliance rules and of criminal liability of those involved, and given the characteristics of the countries to which they export.

- **Supervision of Compliance Programs to Prevent Corruption –** The Director General of the MOD and the Head of DECA are the competent authority for supervising defense exports for reasons of national security, Israel's foreign relations and international commitments, and for maintaining other critical interests; they have the authority to enforce and supervise the implementation of the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions vis-à-vis the defense exporters. Consequently, the Director General of the MOD should determine whether and how the MOD will supervise the defense companies' compliance programs and how they are implemented, as well as what compliance measures small and medium-sized defense companies will be required to implement. It is also recommended that DECA maintain a computer database that compiles information on the existence of compliance programs at defense companies, as revealed in the audits conducted by the department's enforcement unit, to assist with supervision.

- **Statement as part of Agreements Related to Defense Exports –** It is recommended that in agreements related to transactions, the MOD examine what information it wishes to receive about the marketing promoters.

- **Individual Statement to the Defense Establishment Legal Advisor –** The Defense Establishment Legal Advisor should submit to the Director General for approval defined criteria for the requirement of individual statements from relevant position holders at defense exporters concerning the use of marketing promoters.

- **Information about Marketing Promoters –** For optimal supervision and control regarding marketing promoters, DECA should create a complete and detailed database of the people acting as marketing promoters of the defense companies – Israeli and foreign – including the marketing licenses they received or the marketing and export licenses that list their names.

Involvement of the Boards of Directors of Defense Companies in Approving Engagements with Marketing Promoters, including the Fees Paid to Them

- It is recommended that the board of directors rectify the deficiencies identified.
- Given the compliance risks inherent in the use of marketing promoters in export transactions, it is recommended that the Director General of the MOD determine the desired level of involvement of boards of directors at defense companies concerning the use of marketing promoters and the fees paid to them, at least in transactions in which the identity of the marketing promoter requires closer supervision, in accordance with the definitions determined, and in transactions in which the fee – nominally or as a percentage of the transaction amount – is excessive. This should be done to maintain closer supervision by the company's management of this issue in order to reduce the risk of violating the compliance rules to prevent bribery and corruption.

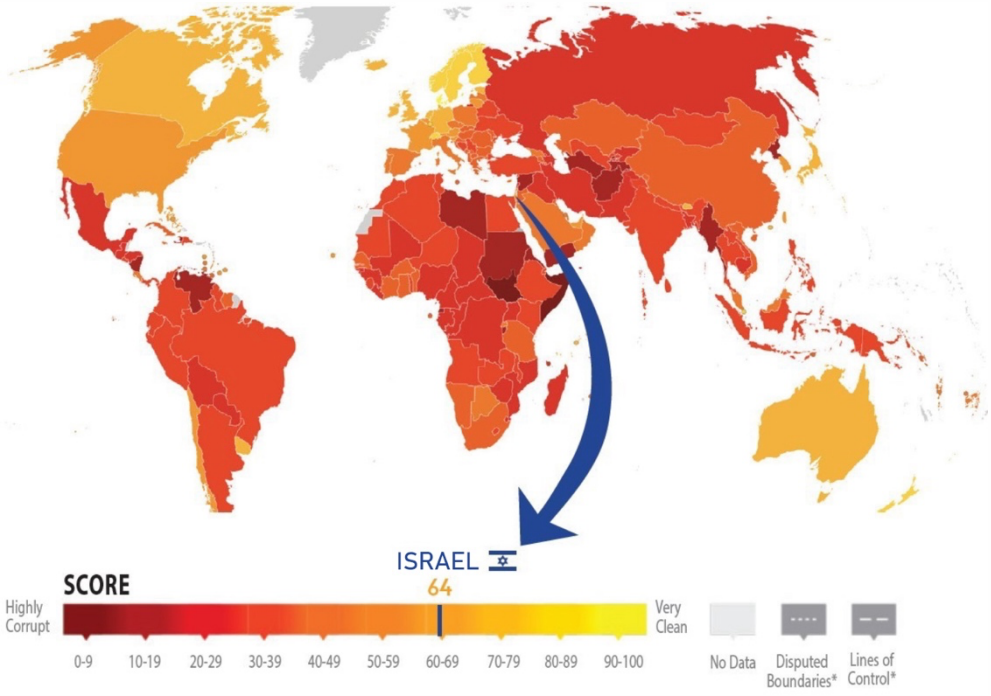
Normative Regulation of Marketing Promoters in the MOD

- **Regulation of Conflicts of Interest in the Activities of Marketing Promoters in Defense Export Transactions –** The defense exporters employ marketing promoters to increase the likelihood of business opportunities developing into transactions. To this end, they also engage with former senior figures in the defense establishment who have connections with current position holders in the MOD. With respect to conflicts of interest between marketing promoters acting on behalf of the defense companies and personnel in the MOD, it is recommended that the ministry receive relevant information directly from the marketing promoters as part of the process of their registration in the registry of exporters and in each request that they make for a marketing license, including their compliance with the Public Service Law (Restrictions After Retirement), 1969. This is for MOD supervision and control over the issue of conflicts of interest of marketing promoters in defense export transactions.
- **Regulation of Fees Paid to Marketing Promoters in the Defense Export Transactions of Defense Companies –** The Director General of the MOD should act promptly to complete the formulation of the ministry's directive on defense export transactions. It is recommended that after the MOD determines the method and criteria for monitoring defense companies' use of marketing promoters in these transactions, including with respect to the fees paid to them and the statements required of defense companies regarding them, it enshrine them in this directive.

  The Defense Establishment Legal Advisor should examine with the Ministry of Justice's Legal Counsel and Legislative Affairs Department the MOD's role in enforcing compliance rules on defense exports at defense companies; subsequently, it should formulate the necessary rules and act to implement them at the MOD.

- **Regulating MOD Employees' Interface with the Defense Companies' Marketing Promoters –** In the ministry's directive that is being formulated, the Planning Department should enshrine the Director General's prohibition against the participation of marketing promoters of defense companies in activities organized by the ministry's departments.
- **Regulating the MOD's Activity to Ensure Defense Companies' Compliance with the OECD Guidelines –** It is recommended that the Planning Department act to enshrine in the MOD's directives all of the necessary actions regarding the prevention of bribery and corruption in defense export transactions and the entities responsible for performing them, including a coordinating body. This should be done so that the State of Israel meets its various obligations on this issue and minimizes its exposure to the various risks involved.

Global Corruption Perceptions Index, 2024



Source: Transparency International website.[14]

14 Corruption Perceptions Index (2024) by Transparency International is licensed under CC-BY-ND 4.0.

Summary

Israel's defense exports greatly contribute to its security, economic growth, and national resilience, and they account for a significant portion of the defense companies' sales. From 2018 to 2023, Israel's defense exports totaled $60.5 billion.

To increase the likelihood of business opportunities developing into transactions, the companies employ marketing promoters. The fees that defense companies committed to paying marketing promoters from 2022 to 2024 totaled hundreds of millions of dollars.

Alongside the benefits that defense companies are likely to obtain from the activity of marketing promoters, their use could also involve significant compliance and regulatory risks related to bribery of foreign public servants. In addition, there is a risk in the use of Israeli marketing promoters who have personal connections with senior figures in the MOD, given the concern that these connections could lead to conflicts of interest and, consequently, to sub-optimal decision-making by the MOD in defense export transactions and to violation of the right to equal opportunity. The materialization of this risk could also undermine public trust in public administration.

The audit found substantial deficiencies regarding the MOD's supervision and control over defense companies' use of marketing promoters, including: the failure to determine rules relating to the supervision of the use of marketing promoters; the failure to determine the measures that small and medium-sized defense companies should adopt to prevent corruption in defense export transactions; the lack of a decision by the MOD on monitoring the compliance programs of defense companies, including the nature and scope of such monitoring; a lack of supervision and monitoring of the identity of marketing promoters; non-regulation of the monitoring of defense companies' use of marketing promoters, including the required level of involvement of boards of directors in approving marketing promoters and their fees; an absence in directives of the actions that the relevant MOD departments must take to implement supervision of defense exports in the context of preventing bribery and corruption and the interactions of MOD employees with marketing promoters in defense export transactions; and the failure of DECA to maintain a complete database of people acting as marketing promoters in defense export transactions and, its consequent failure to supervise all marketing promoters.

The materialization of compliance risks regarding bribery and corruption could significantly undermine the State of Israel's security, foreign relations, and international trade, as well as the reputation of the MOD and of the defense companies involved. Hence, the Director General of the MOD should ensure that the Head of the Planning Department and the Defense Establishment Legal Advisor act promptly to formulate their recommendations regarding the ministry's level of involvement in supervising defense companies' use of marketing promoters in general, including the issue of fees, and it should enshrine the ministry's involvement in its directives. The Director General of the MOD should determine whether and how the MOD should examine the compliance programs of defense export companies and how they are

implemented, and the compliance measures that need to be implemented by small and medium-sized defense exporters.

In addition, to ensure optimal supervision and monitoring of marketing promoters, DECA should create a complete and detailed database of individuals acting as marketing promoters for defense companies – Israelis and foreigners alike – including the marketing licenses they hold or the marketing and export licenses that list their names.

Given the strategic importance of defense exports and their political, military, and economic contribution on one hand, and the risks inherent in defense companies' use of marketing promoters on the other hand, the Director General of the MOD should instruct all departments at the MOD that are involved in this activity, including DECA, the Defense Establishment Legal Advisor, and the Planning Department, to act to rectify the deficiencies found in the audit and according to the recommendations of this report, in order to maintain effective monitoring to reduce exposure to compliance and regulation risks regarding corruption and bribery related to defense exports.