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.

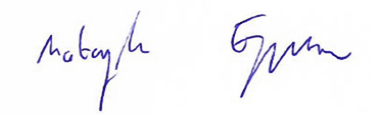
Furthermore, given the centrality and complexity of the funding issue and its importance for advancing the protection of critical facilities in certain entities, the NSC should promptly lead, in cooperation with the Ministry of Defense (which has already begun addressing the matter), the Ministry of 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