Foreword

This report, which is placed on the Knesset's table, presents the results of the audit in the fields of Cyber and Information Technology protection. It also includes a special report on the National Preparedness in the Artificial Intelligence.

Since October 2023, the State of Israel is engaged in the Swords of Iron War, in the north and in the south, following the surprise murderous attack by the Hamas terrorist organization on the communities near the Gaza Strip and the surrounding area on Simchat Torah (celebrating the completion and rebeginning of the reading of the Torah) October 7th, 2023. As I have previously announced, our office is conducting a comprehensive audit on the matters concerning the massacre on October 7th and the Swords of Iron War. In my opinion, it is a public and moral duty to conduct an audit on the manner in which all the echelons functioned on the day of the massacre, during the period preceding it and during the period following it. Alongside with the audit on the war, our office is continuing to conduct audits in other areas as well.

In recent years, and in particular during the course of the war, we are witnessing an increase in cyber-attacks against the State of Israel carried out by states and great powers to damage and disable organizations. The Israel National Cyber Directorate has estimated the costs of dealing with the cyber-attacks in Israel during 2024 at about NIS 12 billion.

When I first took office as the State Comptroller and Ombudsman, I identified and defined the field of cyber as one of the core subjects that the State Audit will deal with. This is with the aim of examining the preparedness and readiness of the audited bodies to deal with the significant risks in the cyberspace, the strategic threats and future cyber challenges. My office's audits in of cyber and information systems indicate the lack of relevant regulation in the cyber field, necessary to oblige organizations to take protection measures; the essential entities in the economy should be prepared to deal with attacks by states or great powers; and the decision makers within the government must be aware of the level of protection in the economy and its deficiencies. This report deals entirely with the results of the State Audit in the cyber and information systems protection. The chapters of the report are as follows:

- **The Government Risk Management in the ICT**
- **Cyber and Data Protection in the National Insurance Institute**
- **The IT Systems in the Israel Postal Company and the Postal Bank**
- **Cyber Protection: Aspects of Regulation and Protection of the Information and Computer Systems at Rafael Advanced Defense Systems Ltd.**

- **The Tevel Project for Upgrading the Computing Systems in the National Insurance Institute – Follow-Up Audit**
- **Ask Once Policy – Follow-Up Audit**

It should be noted that regarding the chapter on the Cyber and Data Protection in the National Insurance Institute and the chapter on the Aspects of Regulation and Protection of the Information and Computer Systems at Rafael Advanced Defense Systems Ltd. confidentiality measures were taken by the Knesset's State Control subcommittee, which decided not to submit them in their entirety before the Knesset but rather publish only parts thereof, under paragraph 17 of the State Comptroller Law, 1958 [Consolidated Version].

The following is an overview of several chapters of the report:

- The digital transformation, which has been integrated into most of the government's work processes, presents opportunities to improve the effectiveness of the government's work and the provision of advanced services to the public, alongside new challenges and risks. During 2022, the scope of the financial activity in the government ICT was NIS 4.8 billion. Therefore, it is essential to manage the risks in this field in an organized and methodological manner. The audit on the subject of **the Government Risk Management in the ICT** indicates considerable gaps in the ICT risk management by the government, including the lack of an overall governmental overview regarding ICT risks; the failure of the National Digital Agency to reduce broad risks; partial reports by government ministries concerning their main ICT risks; and the absence of a main organized and systematic program for ICT risk management in the government ministries, including aspects of risk management regarding projects and broad and cross-cutting risk management – such as a shortage of manpower and difficulty in recruiting and retaining staff. As a result, 80% of the employees in the ICT in the government are freelancers (3,993 out of 5,308 employees during 2022).

  The Israel National Cyber Directorate must address the findings of this audit and the government heat map of the areas of risk in the ICT presented in the audit report, to focus the government activity in this field and ensure that the risk management in this challenging and dynamic field is performed methodologically and optimally and allows preparation for the challenges in advance, providing a solution for the changes occurring in the environment of the government activity.

- The Israel Postal Company was a government company under the full ownership of the State of Israel (until it was privatized in May 2024), providing postal services as well as banking services via its subsidiary – the Postal Bank. As of the end of 2023, the Postal Company and the Postal Bank have 400 postal units, 650 collection centers and about 60 regional postal centers. During 2023, about 11.9 million customers of the Company and the Bank received services in the postal units. The Postal Company has 55 information systems, some of which are divided into sub-systems, and the Postal Bank

has 16 additional systems, some of which are divided into sub-systems, and the annual average of the operational expenses and the investments of the Information Systems Department is NIS 124 million. These systems are based on various technologies and supported by over 20 suppliers. The audit on the f **Information Systems in the Israel Postal Company and the Postal Bank** found deficiencies in the information systems and data protection in the Postal Company and the Postal Bank, including poor management of the procedures for revoking authorizations for employees and its monitoring – thus, 85 (3%) of authorizations holders for a particular system are not defined in the human resources system as "active" and also 79 of them were not located in the Company's computerized controls, 780 (about 13%) of the holders of the active authorizations in the network's central management system are employees who are not included in the list of active employees in the Company's human resources system; the use of outdated automated equipment which is detrimental to both the service provided to the Company's customers and the Bank and the data protection – thus, despite the project for replacing the automated equipment being already defined as a strategic project in 2019, the Postal Company started to replace it only at the beginning of 2022. Until March 2024, only 683 out of 1,850 computers had been replaced or upgraded; the lack of a multi-year work plan for the Information Systems Department; the lack of monitoring and follow-up of the performance of the work plans; the multiplicity of information systems that makes it difficult to transfer the information between those systems and requires the performance of manual procedures and the investment of resources to compensate for this.

The Information Systems Department at the Postal Company must determine a methodological plan that includes the development of the information systems from a future standpoint, the upgrading of old systems and the optimization of the existing systems and the integration between them; while ensuring cyber protection and the reduction of exposure to risks originating in the various aspects of unauthorized use. The Postal Company must, as part of the process improve data protection – and in particular in light of the cyber incident that occurred there in April 2023 – to improve the control over the of Company's authorization management. The Company must examine the deficiencies that were raised in the audit and immediately rectify them.

- The report includes a chapter on the **Cyber Protection: Aspects of Regulation and Protection of the Information and Computer Systems at Rafael Advanced Defense Systems Ltd.** In 2022, the budget allocated to the Cyber and Technology Protection Department at Rafael constituted 10% of the computing budget of the Information Technologies and Processes Administration. Additionally, the rate of phishing incidents reported to the Israel National Cyber Directorate in 2022 represented 31% of the total 9,108 cyber incidents recorded to it that year. The audit identified several deficiencies, including the lack of regulation of the working relationship between the National Cyber Directorate and the Director of Security of the Defense System, as well as deficiencies pertaining to the protection of information and computer systems at

Rafael. It is imperative that Rafael's management and board of directors address these deficiencies and collaborate with the Director of Security of the Defense System to ensure compliance with its directives, as required, given that Rafael's operations are a significant component for the enhancement of the country's military strength and resilience.

- My office conducts follow-up audits to examine whether the deficiencies indicated in the audit reports have been rectified. This report includes the follow-up audits regarding: **The Tevel Project for Upgrading the Computing Systems in the National Insurance Institute** – the follow-up audit indicated that the majority of the core deficiencies that arose in the previous audit had not been rectified or had been slightly rectified. This is notwithstanding that until the completion of the audit, public funds had been invested in the Tevel Project at more than NIS one billion (more than twice as much as the Project's initial overall budget). It was further found that improving the service provided to the public and assisting the public in ensuring its rights had been achieved only partially, among other things due to a reduction in the Project's capacities; **Ask Once Policy** – the follow-up audit found that although since the completion of the previous audit there had been progress in the preliminary activity required for the implementation the Ask Once Policy – most of the deficiencies found in the previous audit had not been rectified with regard to the mapping of the government services provided to the public and an analysis of their characteristics. Although eight years have passed, the government plan resolved upon by the government in 2016 has not yet been fully implemented and the completion of the process is not expected in the next few years. The root of the problem is that the Digital Agency lacks the authority to oblige the government ministries to implement its directives. This, alongside with the lack of engagement of the government and public bodies in implementing those directives, lead to a partial implementation of the Ask Once Policy.

- In addition to the previously detailed chapters of the report, it includes a special report on **The National Preparedness in the Artificial Intelligence**. Preserving the State of Israel's supremacy in the domains of science and technology is a fundamental pillar of its national security, economic resilience, and the well-being of its citizens. This approach strategically compensates for the lack of natural resources and limited human resources compared to other countries. The artificial intelligence revolution is no longer a futuristic concept – it is an innovative core technology that increasingly influences various facets of contemporary life and emerges as a central element of competition in the international arena across a variety of fields: science, economy, industry, security, health, education, and employment.

  The report indicates that the State of Israel already recognized in 2018 that the technological sector is on the brink of a significant revolution, and the Prime Minister acknowledged the necessity of preparing and implementing a comprehensive national plan on the subject. However, the government has not succeeded in leading and executing a broad, comprehensive, and long-term national plan, and implement it, resulting in a decline in Israel's position in international benchmarks attesting to its

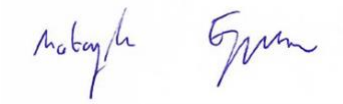
readiness in the artificial intelligence. While the state has identified and analyzed the need in time, for several years it has failed in the decision-making and implementation stages.

To preserve Israel's technological and scientific superiority in the artificial intelligence, deemed a national priority, the Ministry of Innovation, Science, and Technology must guide the government's policy in this field under the government's resolution and the conclusions of the former Minister of Innovation, Science, and Technology in collaboration with the National Security Council. This includes, formulation of the national strategic plan, which was initiated in 2022. Additionally, the Ministry must establish a framework for periodic evaluation of compliance with the established goals in the plan, alongside individual assessments of the defined action directions and necessary updates. Moreover, it is imperative to examine the current management of implementing the approved measures under government resolutions, by parties acting voluntarily and without designated budgetary authority. At this juncture, the Ministry of Innovation, Science, and Technology must assume its responsibilities to ensure that the government's resolution is carried out as required. A clear leadership approach for a significant national program is crucial to maintain technological capabilities and relative advantages over other nations. Any deviation from the prescribed implementation path will necessitate a government update to assess the situation and provide responses to advance artificial intelligence as a government priority. It is recommended that the Prime Minister, who initiated the promotion of a national program in artificial intelligence already in 2018 as a basis for the government's resolution, monitor the government's progress through the National Security Council to ensure the practical implementation of a significant national plan.

It is my pleasant duty to thank the employees of the Office of the State Comptroller, who work devotedly in conducting an audit professionally, intensively, thoroughly and fairly and in the publication of objective, effective and relevant audit reports.

The State Comptroller's Office undertakes to continue auditing the audited bodies' compliance with current and future risks and engaging in cyber defense Information technologies and privacy protection for the benefit of Israeli citizens.

We will continue to pray and hope for the victory of the IDF and the Defense System in this difficult war forced upon us by our most bitter of enemies seeking to destroy us as a nation and as a state, for the return of the hostages to their homes, the return of residents from affected areas in the south and the north to their homes, the recovery of the injured and for peaceful and routine days.



Matanyahu Englman
State Comptroller and
Ombudsman of Israel

Jerusalem, November 2024

State of Israel

Report of the State Comptroller

Cyber and Information Systems

November 2024

Jerusalem | State Comptroller and Ombudsman