OFFICE OF THE STATE COMPTROLLER AND OMBUDSMAN OF ISRAEL

STATE OF ISRAEL

# State Comptroller Report

# Cyber and Information Systems


May 2023

# State Comptroller Report

Cyber and Information Systems

A b s t r a c t s

State of Israel

# State Comptroller Report

## Cyber and Information Systems

## A b s t r a c t s

Office of the State Comptroller | Jerusalem | May 2023

Catalogue Number 2023-S-003

ISSN 0793-1948

www.mevaker.gov.il

Graphic Design: ER Design Team

# Table of contents

## Abstracts

# Foreword

**This report submitted to the Knesset presents the audit's finding in cyber protection, information technology and protection of privacy.**

Technological progress has led more and more areas of our lives to be based on central information systems, and accordingly a considerable frequency increase in the cyber threats and their severity degree is expected. Alongside the advantages of cyberspace for the economy and society, there has been an increase in the cyber-attacks scope, necessitating the strengthening of the protection level and preparedness to cope optimally with cyber-attacks.

Over the past decade, cyber-attacks on organizations and individuals around the world have increased. In 2020, approximately 9.5 million attempted cyber-attacks were detected worldwide, designated to disable computer systems and prevent their use – this year, 18 attempted attacks per minute were detected, on average; In the first half of 2020, at least 36 billion personal data items were stolen or leaked to the internet following cyber-attacks.

At the beginning of my tenure as State Comptroller and Ombudsman, I specified the cyberspace as one of the core issues the state audit will deal with. Examining the preparedness and readiness of the audited entities to cope with the significant risks in cyberspace, with its strategic threats and challenges. This report deals entirely with the state audit's findings regarding cyber protection and information systems. Following are the audits of the report:

a. **Engagements exempted from tender in the ICT Sector**

b. **Accessibility of Government services in the digital age to persons with disabilities and non-users of digital media**

c. **Use of biometric identification documents – identity cards and passports**

d. **Digital technologies and information and cyber security in the Israel Prison Service (IPS)**

e. **Privacy protection and information security in the Center for Collection of Fines, Fees and Expenses systems in the Enforcement and Collection Authority**

f. **Regulation of cyber protection at the National Insurance Institute**

g. **Cyber audit at Medical Center A – penetration test on the infrastructure and the communication network**

It should be noted that the first five audits underwent a classification process, and the Knesset State Audit Committee sub-committee decided not to submit them in their entirety before the Knesset, but to publish only parts thereof, according to Section 17 of the State Comptroller's Law, 1958 [Consolidated Version]. Following is an overview of some of the report's audits:

Reliable identification documents are key to a wide range of operations in the government and business sectors. About a decade before the audit completion, in 2013, a transition to biometric identification documents began in Israel – smart ID cards and biometric passports – meant to replace the old type of identification documents, which are considered easy to forge, and may be used by terror or crime entities and even for illegal immigration. The audit on the **use of biometric identification documents – identity cards and passports** raised that although the transition to smart identity cards began a decade ago for interested residents, and in an obligatory manner for all residents in July 2017, and although NIS 430 million have been invested thus far in issuing them, as of July 2022, millions of residents hold the old type of certificate that is easier to forge. The audit further raised significant deficiencies in several key areas: A significant delay in the transition to biometric national documentation and the failure of use thereof; Deficiencies in protecting biometric data in the computerized systems of the Population and Immigration Authority; and difficulty in coping with the demand increase for biometric identification documents. Given the severity of the audit findings, it is recommended that the Population and Immigration Authority rectify the deficiencies, and that the Minister of Interior ensure the deficiencies rectification in the aforementioned areas, including in the information security and protection in coordination with the professional bodies entrusted with the matter: the Israel Security Agency, the Police, and the National Cyber Directorate. In recent years, there have been far-reaching changes in the national biometric project, including a considerable improvement in the technological capabilities in biometrics, and the scope of online services use that require secure identification has extensively increased. Completing the transition to biometric national documentation, while removing the legal and technological barriers hindering their use and adapting the project to the recent years' changes, may optimize the use of biometric identification documents and is expected to considerably benefit security, economy and public service.

The Israel Prison Service (IPS) is Israel's national correctional organization, a security body included in the law enforcement system and entrusted with the custody of criminal and security prisoners, to protect public safety and security. The IPS is in charge of thousands of inmates and manages a widespread network of correctional facilities throughout Israel, making it a large and complex organization that requires efficient security, management, and technological control resources. This is all the more so due to the organization's sensitive nature and high level of security, as well as the security and criminal risks involved with its proper functioning.

Since 2021, the Israel Prison Service (IPS) has advanced the "Cabinet" program, designed to adapt the organization's technology to its operational and managerial challenges. The audit on **digital technologies and information security and cyber in the IPS** raises significant gaps and substantial deficiencies in a sensitive security system, creating real risks.

A fundamental gap exists between the nature of the organization, its character, the information held by it, and the risks associated with its activity and the functional culture prevalent within it, regarding information security and classified information management. The audit exposes a longstanding reality in which the areas of responsibility and authority of the IPS and the regulators in the information security, cyber, and digital technologies field are not properly implemented as required. Fundamental gaps were found in the disaster recovery plan (DPS) of IPS's technological system.

The status presented in this audit is the result of many years of neglect during which there was no technological governance with defined goals, established processes, allocated resources, and proper management of risks and organizational methodologies in the technological field. There is significant budgetary uncertainty regarding the planned implementation of the response within the "Cabinet" program for the technological and security gaps. It is recommended that the Prime Minister, in consultation with the Minister of Homeland Security, examine the information and cyber security in the IPS in general and, particularly, the classified information security. The IPS and the Ministry of Homeland Security should ensure that functional continuity shall not be compromised by disaster events that could threaten the national correctional system's stability and operation. The Ministry of Homeland Security and its Minister bear responsibility for the functioning of Israel's correctional system; hence, they sould ensure that the IPS fulfills its role through appropriate technological infrastructure, and that force buildup in this field is managed with a long-term perspective and a budgetary framework that guarantees its implementation.

As of November 2022, an average of 2.9 million cyber-attacks are carried out every day at the National Insurance Institute, of which about 66,000 attacks have the potential for harm. Like other countries, Israel is exposed to cyber-attacks for ransom and information theft. Apart from that, given the complex geopolitical climate from a security perspective, Israel is a significant target for potential cyber-attackers, wishing to damage its resilience and national security. The audit on **the regulation of cyber protection at the National Insurance Institute** raised that an entity such as the National Insurance Institute requires a satisfactory regulatory response formulated for it, including guidance from the National Cyber Directorate, from the Privacy Protection Authority, and coordination between the two to ensure optimal protection. Given the volume of information kept at the National Insurance Institute and the leaking risks, it is recommended that the Supreme Steering Committee, authorized to consider bodies defined as critical and therefore in need of cybernetic protection, will promote the examination of the National Insurance Institute as a critical cyber infrastructure (CCI) entity. It is recommended that until the examination is completed, a professional interface will be regulated between the National Cyber Directorate and the National Insurance Institute to provide a direct response, transmit reports, control the deficiencies rectifications, etc. It is also recommended that the Steering Committee consider other entities that have databases of similar scope to the National Insurance Institute whose definition as CCI entities should be examined, thus improve the protection of the State of Israel's critical infrastructures.

The audit on **privacy protection and information security in the systems of the Center for Collection of Fines, Fees and Expenses at the Enforcement and Collection Authority** raises deficiencies in privacy protection and information security in the information systems at the Center for Collection of Fines of the Enforcement and Collection Authority, even though its operational system is defined as a database requiring a high level of security. Among the deficiencies that arose: the lack of access documentation of the Center's operational system users to its information, resulting in a lack of control over that access; Failure to adequately monitor unusual events in the system; Inadequate management of the privileges granting process to the Center's operational system and of the supervision and control over them; Unlimited access of the system users to its information; Inadequate management of the telephone information center employees' system privileges; As well as the risk of outside attackers infiltrating the Center's systems. The Enforcement and Collection Authority and the Center for Collection of Fines should act under the instructions of the relevant bodies, at the earliest possible time, to prevent information leaking from the organization and to maintain its integrity. The Center for Collection of Fines' database is wide-ranging and includes sensitive information of about 3 million debtors. The debt handled by the Center for Collection of Fines is about NIS 6.8 billion as of the audit date. Hence the need to protect the information systems, to prevent damage to the integrity of the information and to the functional continuity of the Center for Collection of Fines, prevent the data and information leaking from the database and prevent their disclosure to unauthorized parties.

In recent years, cyber threats to the health system, including medical centers, have also increased. Furthermore, the health sector was one of the ten most attacked sectors in Israel in 2021. One of the methods to contend with cyber threats is to perform penetration tests on the organization, to identify vulnerabilities in its defense and mitigate them. When it is not possible to address the vulnerabilities that have arisen, the potential risks should be presented to the organization's management and handled on an ongoing basis. This report includes a **cyber-audit at Medical Center A – a penetration test on the infrastructure and the communication network.** In the penetration test, 13 significant findings were identified in five areas: Segmentation and flow control; Network access control; Protection of workstations and servers; Out-of-date software; And unsecure access. Ten of the findings were of high severity and three of moderate severity. Following the penetration test, the management at Medical Center A rectified several deficiencies, and in particular updated the security level of certain systems. According to the Medical Center's management, the total cost of rectifying the deficiencies may excess NIS 10 million per annum on an ongoing basis. It is recommended that the management formulate an organization-wide work plan to eradicate the risks or to mitigate them in cases where it is not possible to rectify the deficiencies that have arisen. It is further recommended to carry out penetration tests according to a regular plan. The Ministry of Health as the regulator of the medical institutions, including in information security should execute penetration tests it has begun to perform in all medical institutions in Israel and establish a periodic format to continue penetration tests in the institutions. It is further recommended that the Ministry of Health examine the findings of the Medical Center A

penetration test and implement them in all medical institutions. Moreover, it is recommended that the Ministry of Health ensure that all the medical institutions themselves perform periodic penetration tests, examine the findings of these tests, monitor the rectifying of the deficiencies that arise and, accordingly, publish recommendations to all the medical institutions. In addition, it is recommended that the Ministry of Health continue to help all medical institutions at the national level to cope with the medical devices information security challenges.

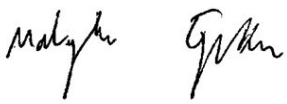
Government procurement is a central pillar in the activity of government bodies since most government activity depends on the procurement of goods or services. The audit on **engagements exempted from tender in the ICT Sector**, raised that the scope of ICT procurement in 2019–2021 was about NIS 14.4 billion, about 15.6% of the total government procurement in these years. The scope of ICT procurement carried out through tender exemption in 2019–2021 was about NIS 1.79 billion, about 14.2% of the total ICT procurement in those years. The findings of this report indicate a series of deficiencies in procurement, particularly ICT engagements exempted from tender. Following are the key deficiencies: The information published to the public by the Procurement Administration and the National Digital Agency in procurement does not match the information held in the Merkava (Comprehensive Lateral System in Government Ministries) system, thus compromising transparency to the public and the ability to control government procurement activities; The government bodies use of the tender exemption on the grounds of a single supplier or an engagement of up to NIS 50,000 in ICT procurement is hundreds of percent greater than such use in general procurement; And non-compliance with the publication of engagements law provisions. The rapid development of the ICT field obligates government bodies to implement innovation in this field quickly and efficiently, to prevent the technology from becoming obsolete by the time the procurement process is completed. Alongside, procurement procedures should be managed in a fair, equitable and transparent manner and under the provisions of the law to accomplish business results and economic efficiency. The governmental bodies should adhere to the provisions of the law and of the government procurement Directives on Regulation, Finance and Economy (TAKAM Directives). It is recommended that the Procurement Administration improve the procurement process in the Merkava system, implement computerized controls and compensatory controls, to verify the integrity and reliability of the information and to improve the ongoing supervision and control and the decision processes. The Accountant General and the Freedom of Information Unit should enforce the publication of the engagements of all entities under the provisions of the law, while ensuring the reliability of the information published to the public.

The audited entities have the duty to rectify quickly and efficiently the deficiencies raised in this report, to raise the organization's level of protection and to handle optimally cyber-attacks. The entities should adapt their activities to a world saturated with advanced technologies and to future challenges. The recent cyber-attacks highlight the need for this.

**Finally, I have the pleasant duty of thanking the employees of the State Comptroller's Office, who work dedicatedly to conduct professional, in-depth,**

**thorough and fair audits and to publish objective, effective and relevant audit reports.**

The State Comptroller's Office undertakes to continue audit the entities' withstanding of current and future risks and engage in cyber protection, information technologies and privacy protection, for the benefit of the citizens of Israel.



**Matanyahu Englman**
State Comptroller and
Ombudsman of Israel

Jerusalem, May 2023

State Comptroller's Report – Cyber and Information Systems | May 2023

Systemic Topics

# Engagements Exempted from Tender in the ICT Sector

# Engagements Exempted from Tender in the ICT Sector

## Background

Government procurement is a central pillar in the activity of government bodies since most government activity depends on the procurement of goods or services. An efficient government procurement system ensures proper conduct and optimal utilization of public funds. Streamlining ICT procurement, based on technology that changes frequently, is essential for promoting ICT and technological innovation in government bodies. The transparency of procurement procedures in the government is of great importance, both from a Moral Perception of responsibility for public funds and from a professional aspect, according to which a transparent and competitive procurement process will bring better results for the government bodies. In June 2022, a draft was published for public comments regarding the amendment to the Mandatory Tenders Regulations, 1993.

The scope of ICT procurement in 2019–2021 was about NIS 14.4 billion, about 15.6% of the total government procurement in these years. The scope of ICT procurement carried out through exempt from the tender in 2019–2021 was about NIS 1.79 billion, about 14.2% of total ICT procurement in those years.

## Key Figures

**NIS 14.4 billion**
the scope of ICT procurement in 2019–2021

**NIS 4.2 billion**
the gap between the procurement scope in 2020 presented in Merkava system and the scope published by the Government Procurement Administration

**NIS 1.79 billion**
the total ICT procurement exempt from the tender in 2019–2021 (14.2% of the total ICT procurement in those years)

**717**
the number of ICT purchase orders in the range of NIS 47,500–50,000 through an exemption from the tender on the grounds of "purchases up to NIS 50,000"

**25%**
of the government bodies did not submit the required reports for 2021 to the Government Freedom of Information Unit

**40%**
of the contracts exempt from tender publicized, lack essential information required by law

**61%**
of the ICT engagements exempt from tender on the grounds of a "sole source purchase" (NIS 1.1 billion)

**Six-fold**
the government bodies' use rate of the "sole source purchase " exempt in ICT procurement (61%) is six-fold than the one in non-ICT government procurement (9.72%)

# Audit Actions

From April to October 2022, the State Comptroller's Office examined government bodies' ICT engagements through an exemption from a tender. The audit was conducted in the Accountant General's Division of the Ministry of Finance (the Accountant General). It was based on data retrieved by the State Comptroller's Office from the Merkava (Comprehensive Lateral System in Government Ministries) system, the website of the Procurement Administration at the Ministry of Finance, and the Government Freedom of Information Unit website. Completion examinations were conducted at the Ministry of Welfare and Social Security, Construction and Housing, the National Digital Agency at the Ministry of Economy and Industry (the National Digital Agency), the Israel Mapping Center, and the Competition Authority.

# Key Findings

**ICT Engagements Through an Exempt from Tender on the Grounds of a "Sole Source Purchase " –** ICT procurement through an exempt from tender on the grounds of a sole source purchase in 2019–2021 was NIS 1.1 billion – about 61% of the total ICT procurement through an exempt from tender, this compared to a corresponding rate of 9.7% in general procurement (without ICT).

- It was found that the use of the sole source purchase exemption by the government bodies in ICT procurement (61%) was over six-fold than in non-ICT government procurement (9.72%).

- It was found that the government procurement system has eight suppliers when two-thirds and more of the ICT procurement orders (in monetary terms) issued to them, at about NIS 130 million, were exempted from the tender on the grounds of a sole source purchase. Furthermore, six suppliers with which the sum of the engagements, exempt from the tender on the grounds of a sole source purchase, was the largest – about NIS 467 million. It should be noted that engagements were also made with those suppliers through tender procedures. This may raise concerns regarding the lack of perfect competition and the violation of the principle of equality under the principles established by law, as well as the non-exhaustion of the examination of the alternatives by the government body before the decision to use the exemption on the grounds of a sole source purchase.

- It was found that in four government bodies – the Ministry of Transport and Road Safety (Ministry of Transport), the Ministry of Agriculture and Rural Development, the Labor Division of the Ministry of Economy and Industry, and the Israel Tax Authority (the Tax Authority) – the average rate of ICT procurement through an exempt from tender on the grounds of a sole source purchase in 2019–2021 is almost double to more than double the average rate of ICT procurement that is carried out without a tender in all government ministries (14%) (Ministry of Transport – 31%; Ministry of Agriculture and Rural Development – 31%; Labor Division of the Ministry of Economy and Industry – 27%; Tax Authority – 26%). The total of the ICT procurement through an exemption from the tender on the grounds of a sole source purchase in the four entities was about NIS 627.7 million.

- In an examination of 65 minutes of ministerial committees convened in 2019–2021, it was raised that in the vast majority (97%) of the professional opinions submitted to the tender committees, the measures taken to locate additional suppliers were not detailed as required under the provisions of the Directives on Regulation, Finance, and Economy (TAKAM Directives). Without this information, the

committee's ability to reach the certainty required to approve the request is significantly impaired.

- The audit raised that the Procurement Administration does not have comprehensive information on the objections to engage through an exemption from the tender on the grounds of a sole source purchase, and in practice, each government body handles separately the objections submitted to it on its intentions to engage on these grounds. The presence of comprehensive information on the objections submitted to the government bodies on the engagement exempt from tender at the government body in charge of government procurement – will improve its decisions regarding optimizing the government procurement processes.

**ICT Engagements Through an Exempt from Tender due to a Contract Sum of up to NIS 50,000 –** in 2019–2021, ICT procurement orders through an exempt from tender due to an engagement of up to NIS 50,000 (Regulation 3(1)) were NIS 161 million, about 9.1% of the total ICT procurement orders through an exempt from tender in these years, compared to a corresponding rate of 2.8% in general procurement (without ICT).

- Nine cases were found, at NIS 898,000, in which several procurement orders from the same supplier for the same service were made within up to 14 days, each in less than NIS 50,000, but cumulatively they were over this sum. Artificial splitting of engagements, if done, violates the principle of equality based on the tender laws. The obligation to carry out the procurement through a tender is circumvented through it. Furthermore, due to fragmentation, public funds may be overused due to the non-utilization of the size advantage.

- Regarding procurement orders classified as engagements exempt from tender under Regulation 3(1) made in the range of NIS 25,000–50,000, it was found that in 2019 – 2021 717 procurement orders were made in the range of NIS 47,500–50,000 – the most significant number of procurement orders from all the sum tiers included in the range of NIS 25,000–50,000. The number of procurement orders in the second largest sum tier was 202. That is, the number of ICT procurement orders classified as engagements exempt from tender under Regulation 3(1) and carried out in sums close to the exemption cap set in the regulations is three-fold than the number of procurement orders in any other sum tier.

- Moreover, it was found that the Prime Minister's Office executed about 22% (156) of the 717 procurement orders, the Central Bureau of Statistics executed about 7.5% (53), the Ministry of Justice executed about 7.3% (52), and the Ministry of Health executed about 5.9% (42). It was also found that there are three suppliers with whom the number of engagements made by the government bodies in this

price range constituted over 40% of all engagements with them in 2019–2021. This raises the concern that government bodies sometimes adjust procurement orders to the sum exempted from the tender. Due to the reduction of the quality or quantity of the procurement to avoid a tender, a waiver of requirements necessary for the activity of the governmental body is possible. Furthermore, the ability to plan the procurement may be adversely affected due to the absence of a complete situation report of the government body's procurement needs.

**Publication of Government Engagements**

- It was found that in about 40% (about 7,000) of the publications of engagements through an exempt from the tender in 2019–2021, the government bodies did not publicize all of the information (the name of the supplier, The value of the engagement or an estimate thereof; The dates of the start and end of the engagement) in contravention of the legal requirements when engaging with suppliers through an exempt from the tender. This affected the transparency to the public and the Procurement Administration's control ability.

- Regarding the completeness and reliability of the data published in the engagements report, it was raised that in hundreds of cases, material errors were found in the details of the engagements: in six cases, the engagements were categorized as exempted on the grounds of being up to NIS 50,000, even though the scope was over this sum; In 822 cases the engagements were categorized as exempted when the required approving party according to this ground for exemption is different than the party specified as the approving party; In 585 cases the engagements were categorized as exempted on the grounds of a sole source purchase, while the relative professional opinion was not attached, as required under the provisions of the Directives on Regulation, Finance, and Economy (TAKAM). These could have been avoided if there were basic controls in the publication module alerting the government bodies of errors or deficiencies in the data entry.

- It was found that in 2019–2021, the government bodies submitted an average of 62.5% of the reports on the date set by the directives of the Freedom of Information Unit. In contrast, over a third of the bodies (37.5%) did not submit a report or submitted it late. The delay ranged from a few days to a few months. This is in contravention of the Unit's directives and the government's resolution to promote transparency and expand the proactive dissemination of information for the benefit of the public.

- Regarding 70 ICT procurement orders by the Ministry of Transport in 2019–2020, 9 (13%) of them, for about NIS 3.3 million, were not published on the Freedom of Information Unit website. Regarding 135 ICT procurement orders executed by the

Ministry the Health in 2019–2020, 7 (5%) of them, at about NIS 5.2 million, were not published on the Freedom of Information Unit website.

- **Information Published by the Procurement Administration in the Annual Government Procurement Reports –** the Procurement Administration presents, in its annual report, the comparative data of the previous year based on the data published in the previous year and not based on a new retrieval intended to obtain current data. As a result, updates made by the government bodies to procurement orders created in subsequent years do not appear in the Procurement Administration data. It was found that there are gaps of NIS 1.2–4.2 billion between the scope of procurement presented in the Procurement Administration's report for 2019–2020 (NIS 27.3 billion and NIS 30.5 billion, respectively) and the scope of procurement for these years in the data of the Merkava (Comprehensive Lateral System in Government Ministries) system as of June 2022 (NIS 28.5 billion and NIS 34.7 billion, respectively).

- **Categorization of ICT Procurement in the Merkava (Comprehensive Lateral System in Government Ministries) System –** Merkava does not have defined rules or a binding government directive for the use of SKUs or specific groups of material enabling to identify all or some of the ICT procurement operations. It was also raised that Merkava does not have a compensatory control, such as a computerized control mechanism to warn of using SKUs that do not match the procurement group or to prevent this use. Therefore, government bodies cannot obtain a current and accurate ICT procurement situation report through computerized means. In addition, the supervisory and control bodies – the Accountant General, the Procurement Administration, and the National Digital Agency – cannot receive comprehensive information on ICT procurement in all government bodies. For example, the Central Election Committee entered into the Merkava system in 2019–2021 procurement orders at NIS 227 million for payments to the Knesset factions for their representatives' attendance at the polling stations. These orders were categorized by Merkava as "computer services," even though they are payments to factions. In other words, the ICT procurement analysis, including the "computer services" category, would have created a significant bias in the data.

- **Built-in Controls in the Merkava System –** Merkava lacks some built-in controls that could have prevented errors made as part of the execution of a procurement order through an exempt from tender, or that could have alerted such errors, such as classifying procurement orders as exempt from tender due to an engagement with a government company, even though the engagement is with a private company; Classification of procurement orders as exempt from the tender on the grounds of engagement of up to NIS 50,000, even though the order sum is more significant. It even reaches hundreds of thousands and millions of NIS.

- **National Digital Agency Information on the Scope of ICT Procurement –** the managers of digital and information technology departments manually enter into the Agency's dedicated system the data on which the National Digital Agency bases the

report. These data are not linked to the Merkava data, and in practice, there are gaps between the information reported by the Agency and the data in the Merkava system. The sums reported in the Agency may be larger or smaller than the data in the Merkava system. The audit raised gaps of NIS 1.2–1.4 billion per year between the sums published by the National Digital Agency each year, and the sums in Merkava, defined as ICT procurement by the State Comptroller's Office.

**Classification of Engagements as Sensitive –** the State Comptroller's Office sampled 25 procurement orders from among the ICT engagements of government bodies in 2019–2021 through an exemption from tender and classified as sensitive. It was found that 5 (20%) of them, at NIS 390,000, were unnecessarily classified as sensitive and were not published on the government Freedom of Information Unit website.

**The Procurement Administration's Activities to Strengthen Transparency –** the State Comptroller's Office commends the Procurement Administration website strengthening the transparency of various aspects of government procurement, including the engagements through an exemption from a tender. Such as, the publication of general information on the Procurement Administration's activities, the publication of reports, and the creation of a dashboard and a database of questions and answers.

# Key Recommendations

The Procurement Administration should examine the gaps between the procurement data in its publications and the data on procurement carried out in practice in a particular year as presented in the Merkava (Comprehensive Lateral System in Government Ministries) system. It is also appropriate to examine whether the Procurement Administration presents a complete and updated situation report of the procurement carried out in practice each year, and not rely on data entered in previous years that, as stated, do not reflect the actual procurement.

Due to the procurement scope in general, and the ICT procurement scope in particular, the Procurement Administration and the Merkava unit, in cooperation with the National Digital Agency, should establish an outline computer classifing the ICT ministerial and the governmental expenditure. Establishing a computerized reporting mechanism to receive reliable information from various governmental bodies is also appropriate. Thus, the situation report of the governmental ICT activity will reflect the actual procurement and will be compatible with the procurement data in the Merkava system.

- It is recommended that the Procurement Administration and the Merkava unit implement structured controls in the Merkava system and appropriate compensatory controls to prevent and detect errors in the entry of procurement data to the Merkava system, reliably presenting the data to the public and in the analysis of the data by the government bodies and the Procurement Administration.

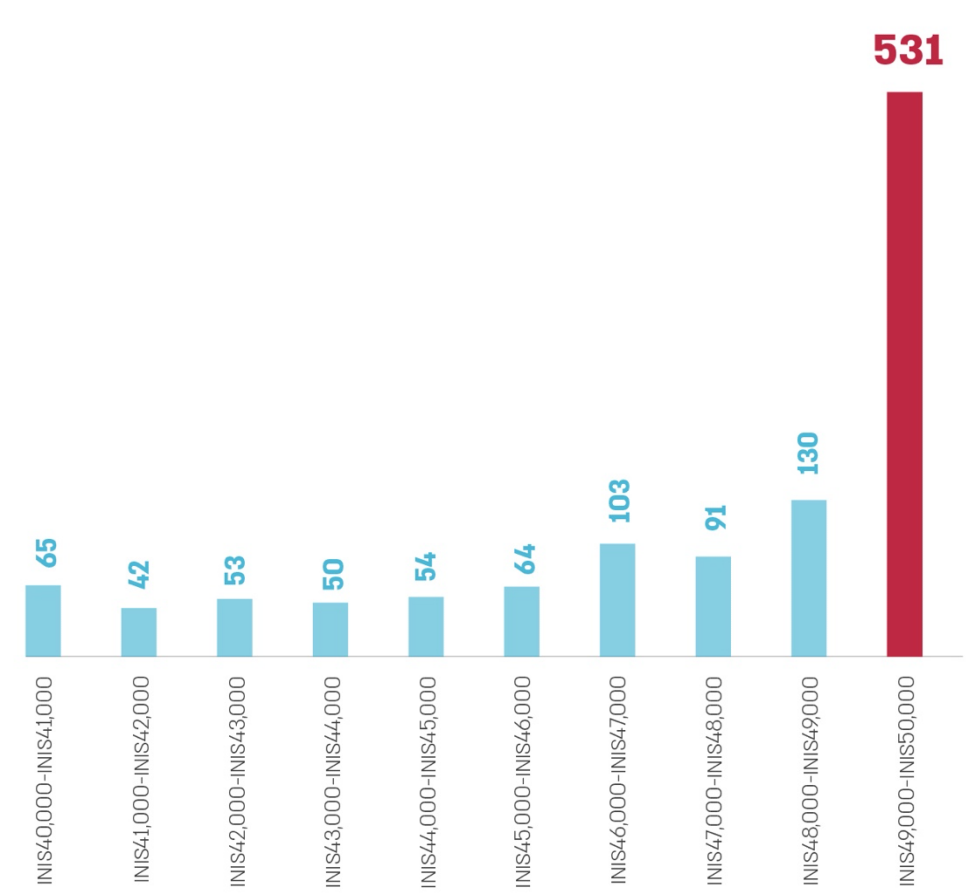
- It is recommended that the Accountant General examine individually the engagements of the government bodies with the suppliers, most of which through exemption from the tender on the grounds of a sole source purchase, and the engagements with the suppliers whose scope of the exemption from tendering, for this reason, reaches tens and hundreds of millions of NIS. It is further recommended that the Accountant General employ digital tools for continuously monitoring multiple purchase orders from the same supplier with an exemption on the grounds of a sole source purchase and consider intervention in the appropriate cases. It is also recommended that the Procurement Administration consult, to the extent necessary, with the Competition Authority regarding examining the findings raised and improving perfect competition.

- It is recommended that the Accountant General control the implementation of the guidelines among all government bodies in these matters: (a) The level of detail required in the professional opinion from each ordering unit, including the attachment of documents on the examinations, carried out and their results; (b) The degree of certainty required from the ministerial committees before approving engagements on the grounds of a single supplier. It is appropriate that according to the outcome of the control, the Accountant General will consider refining its guidelines. It is also appropriate that the Accountant General characterize a digital tool compiling all the objections received in the various procurement procedures in the ministries and present to the Procurement Administration cases of multiple objections to a particular supplier, of numerous objections on a specific object of an engagement or of multiple objections on the intentions of a particular body of government so that the Administration can use the tools at its disposal according to the need regarding the decision on exemption from tendering for the government ministries, the creation of agreed terms and prices, passing on dedicated instructions to the tender committees and more.

- It is recommended that the government bodies ensure that the procurement requirements are not reduced in quantity or quality and do not try to circumvent tendering in this way. It is also appropriate that the Ministry of Finance complete the amendment to the regulations, including raising the threshold requiring the execution of procurement through a tender, which at the audit completion was NIS 50,000. It is further recommended that the Procurement Administration consider additional controls on engagements made in sums close to the exemption cap to ensure no reduction in quantity or quality and examine the need for holding a central tender for computer products purchased in sums close to the exemption cap.

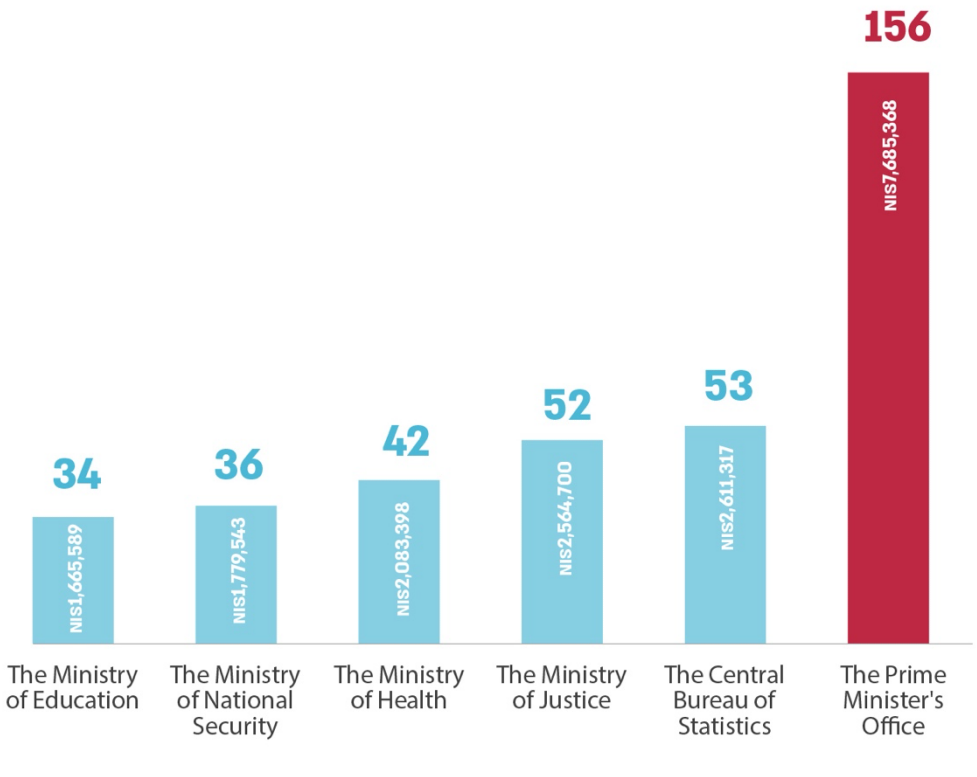
The governmental bodies should ensure complete and accurate publication of the data of the engagements under the provisions of the TAKAM Directives. The Freedom of Information Unit, in cooperation with the Accountant General, should enforce the publication of the engagements of all entities within the stipulations set in the Freedom of Information Law. It is also recommended that all the parties involved – the Procurement Administration, the Merkava (Comprehensive Lateral System in Government Ministries) Unit, and the Freedom of Information Unit – consider establishing computerized interfaces between the systems to ensure an accurate presentation of the government engagements.

**The Frequency of ICT Purchase Orders Through Exempt Under Regulation 3(1) at NIS 40,000–50,000 NIS, in Increments of NIS 1,000, 2019–2021**




According to the Merkava data processed by the State Comptroller's Office.

## The Scope and Number of ICT Purchase Orders Through Exempt Under Regulation 3(1) at NIS 47,500–50,000 by Government Bodies that Made at Least 30 Orders, 2019–2021




According to the Merkava data processed by the State Comptroller's Office.

# Summary

The rapid development of the ICT field means that government bodies should implement innovation quickly and efficiently to prevent the relevant technology from becoming obsolete until the procurement process is completed. At the same time, the public interest requires that the procurement procedures be conducted in a fair, equitable, and transparent consistent with the provisions of the law and lead to business results and economic efficiency.

The findings of this report indicate a series of deficiencies in procurement, with an emphasis on ICT engagements exempt from tender. The following are the main deficiencies: the information published by the Procurement Administration and the National Digital Agency in procurement does not match the information in the Merkava system, thereby compromising the transparency to the public and the control capabilities of government procurement activity; Hundreds of percent higher use of government bodies of the exempt from tender on the grounds of a sole source purchase and on the grounds of engagements in sums up to NIS 50,000 in ICT procurement, compared to general procurement; And non-compliance with the provisions of the law concerning the publication of engagements.

The government bodies should adhere to the provisions of the law and the government procurement provisions of the TAKAM Directives. It is recommended that the Procurement Administration improve the procurement process in the Merkava system, including implementing computerized controls and compensatory controls, to verify the information's completeness and reliability and improve the ongoing supervision and control and the decision-making processes. The Accountant General and the Freedom of Information Unit should enforce the publication of the engagements of all entities under the provisions of the law while ensuring the reliability of the information made available to the public.

State Comptroller's Report – Cyber and Information Systems | May 2023

Systemic Topics

# Accessibility of Government Services in the Digital Age to Persons with Disabilities and Non-Users of Digital Media

# Accessibility of Government Services in the Digital Age to Persons with Disabilities and Non-Users of Digital Media

## Background

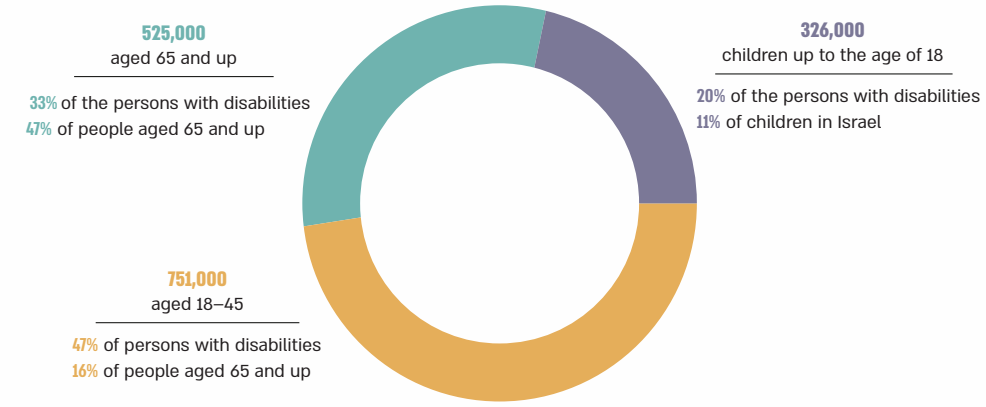
Government bodies provide services to the public through various channels, including public reception bureaus, service call centers, and digital channels (their websites and apps). Technological development has led to the public's increased use of digital means when consuming information and services and contacting public bodies through digital service channels. The use of digital channels enables the government to optimize service to the public and save labor inputs since the cost of face-to-face service is 50 times higher than the cost of digital service. This use also reduces the bureaucratic burden imposed on the public, making the government service more available, convenient, and consumed from anywhere and at any time. The Equal Rights For Persons With Disabilities Law, 1998 (the Law), and the regulations promulgated thereunder, establish provisions for service accessibility for persons with disabilities, including the service provided through digital channels. Various entities that provide services to the public, including government bodies, should make the information and the services they provide to the public through digital channels accessible for persons with various types of disabilities. Full accessibility to the extent possible of the digital government service is necessary for the public as a whole, particularly for persons with disabilities, so that they, too, can use it in a dignified, equal, and independent manner. The need for making digital services accessible to the public, and in particular to persons with disabilities, becomes even more critical during times of emergency, for example, during a pandemic such as the Covid-19 pandemic or in times of war, as in such times the digital channel becomes the main channel where information and services can be obtained.

Another aspect that government bodies should address in the current era, characterized by the expansion of digital services, is the need to preserve non-digital service channels – service at public reception bureaus, by phone and by mail, to allow people and population groups that rarely use the internet nor consume government services through digital channels, or even avoid doing so, also to receive the services in an available and convenient way. At the same time, government bodies should identify the barriers that prevent such people from using their digital service channels and remove these barriers for them or at least minimize them.

## Persons with Disabilities in Israel, Triennial Estimates (2018–2020)

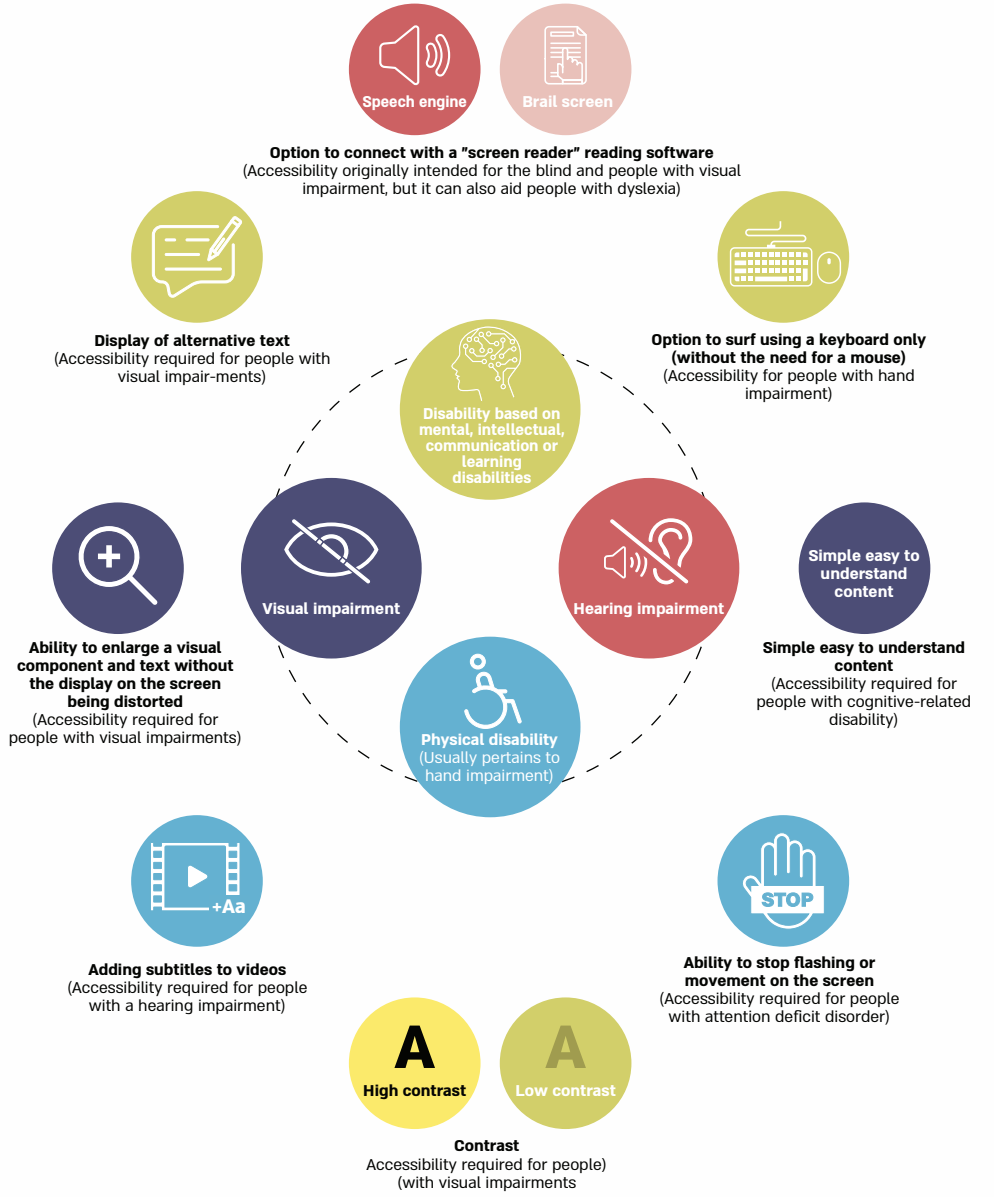
In Israel there are about 1.6 million persons with disability

Triennial estimates based on the Social Survey after non-response corrections and the addition of popula-tions not included in it




According to the Myers-JDC-Brookdale Institute data processed by the State Comptroller's Office.

## Types of Disabilities that Require Digital Accessibility and the Main Accessibility that can be Provided



## Key Figures

**57%**

of the 23 government bodies that participated in the State Comptroller's Office survey (13 bodies) reported that they did not make accessible all the required content and services on their main website

**43%**

of the 23 government bodies that participated in the State Comptroller's Office survey (10 entities) have not yet performed an accessibility check of their website, once every five years, as required

**in 100%**

of the 15 websites of 14 government bodies, which the State Comptroller's Office sampled and checked accessibility, found items that were not made accessible to persons with various disabilities, as required by the Law

**about 50%**

of the government bodies that participated in the State Comptroller's Office survey (12 out of 23 bodies) made available on their public websites, only part of the required documents under the provisions of the Law

**100%**

in each service process in the 16 digital government service pages most viewed, the State Comptroller's Office found at least two items that were not adequately accessible to persons with disabilities

**39%**

of about 520 persons with disabilities who use the internet in their daily lives reported in the State Comptroller's Office survey that they encountered inaccessible items on websites or applications (apps) of government bodies, as required

**31%**

of the people who rarely consume government services online or who refrain from doing so reported in the State Comptroller's Office phone survey that they encountered instances where they wished to receive a government service through non-digital channels (public reception bureaus, phone or mail), and it was not possible because they were required to have a means they did not have, such as an e-mail, an internet connection or a credit card

**38%**

of about 520 persons with disabilities reported in the State Comptroller's Office survey that they encountered instances where it was impossible to receive service from government bodies except digitally (I.e., they could not consume the service by phone or at a public reception bureau)

# Audit Actions

From January to October 2022, the State Comptroller's Office audited the accessibility of digital services to persons with disabilities and the response provided to non-users of digital media or to people who seldom do so for the receipt of government services. Below in the diagram is a breakdown of the audit topics, the types of audited bodies, and the methodology used in this audit.

Government bodies in which the State Comptroller's Office conducted accessibility checks on their websites or who responded to its survey are the National Insurance Institute, the Ministry of Religious Services, the Small and Medium Enterprises Authority (ISMEA) – the Ministry of Economy and Industry, the Central Election Committee, the Israel Knesset, the Courts Administration, the Israel Police, The Ministry of Defense (the Rehabilitation of Disabled Veterans Department website), the Ministry of Construction and Housing, the Ministry of Health, the Ministry of Foreign Affairs, the Ministry of Education, the Ministry of Agriculture and Rural Development, the Ministry of Justice, the Ministry of Interior, the Ministry of Welfare and Social Security, the Ministry of Transport and Road Safety, the Ministry of Tourism, the IDF (Meitav Unit website)[1], Israel Railways, the Enforcement and Collection Authority, the Population and Immigration Authority, the Nature and Parks Authority, the Tax Authority, the Israel Land Authority, the Securities Authority, the Airports Authority and the Employment Service.

1 Meitav is a unit engaged in recruiting, screening, placement and deployment issues. https://www.mitgaisim.idf.il

# The Audit Topics, the Types of Audited Bodies, and the Methodology, 2022

2022

October — January

## The audit topics

The response given to non-users of digital media

Accessibility of the digital services of government bodies to persons with disabilities

## Audited Bodies

**03**

**Government Bodies**

1. An audit was carried out on the websites of 14 government bodies
2. A survey was carried out in which a questionnaire was sent to 23 government bodies who answered it

**02**

**Commission for Equal Rights of Persons with Disabilities**

(Ministry of Justice)

**01**

**The National Digital Agency**

(Ministry of Economy and Industry)

The audit was carried out at the MyGov Unit and at the Improvement of Government Service to the Public Unit

## Methodology

### Audits in government bodies

**Examination of accessibility** on the bodies' websites

15 websites of government bodies

**Examination of accessibility** to the service pages most viewed by the public

16 online government service pages

**Survey** concerning accessibility on websites and apps

23 government bodies responded

### Public participation processes for receiving information on customer experience

**Phone survey**

Among people who do not consume government services online or who do not use the digital service channels at all

301 people aged 60 and up responded | Ultra-orthodox and Arab

**Online survey**

The survey was distributed to persons with disabilities using the internet

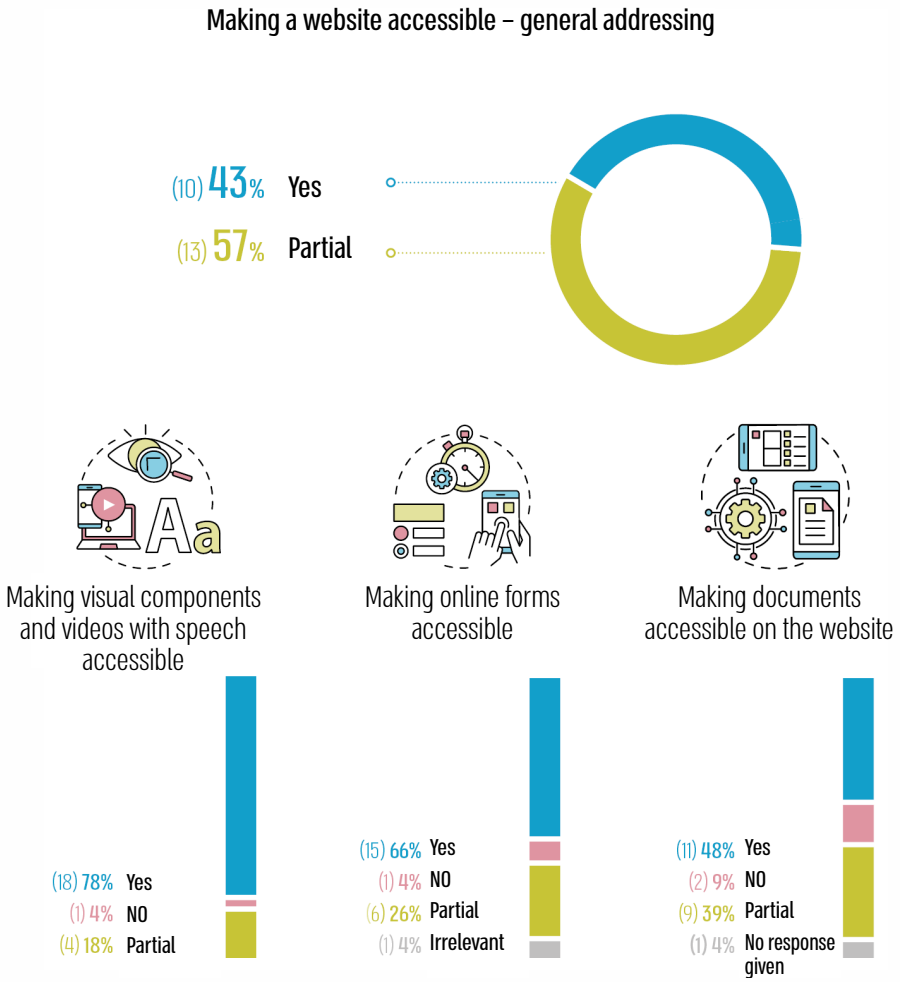
527 people responded

# Part One: Digital Accessibility for Persons With Disabilities

## Key Findings

- **Survey Findings – Accessibility of Government Bodies Websites –** the State Comptroller's Office survey findings among 23 government bodies raised that the websites of 13 of them (57%) do not meet the accessibility requirements prescribed by law. Some items are not accessible to persons with various disabilities, even though making them accessible is required. The websites belong to the following bodies: the Nature and Parks Authority, the Ministry of Interior, the Ministry of Transport and Road Safety, Israel Railways, the Enforcement and Collection Authority, the Ministry of Health, the Ministry of Education, the Courts Administration, the Central Election Committee, the Israel Land Authority, the Ministry of Religious Services, the Ministry of Foreign Affairs and the Ministry of Tourism.

## Reports by Government Bodies on their Websites and some Items Accessibility*




* "Yes" – Fully accessible (all items included in this category have been made accessible); "Partial" – Only some of the items belonging to each component (category) were made accessible; "No" – No actions for making it accessible were carried out; "No response given" – The body did not provide information in its answer to the survey; "Irrelevant" – The component type does not exist on the entity's website.

**Periodic Accessibility Checks –** 10 out of 23 government bodies (43%) that participated in the State Comptroller's Office survey – the Ministry of Welfare and Social Security, the Israel Land Authority, the Ministry of Construction and Housing, the Ministry of Religious Services, the Enforcement and Collection Authority, the Ministry of

Agriculture and Rural Development, the Courts Administration, the Ministry of Foreign Affairs, the Israel Police as well as the Tax Authority – have not yet conducted a periodic accessibility check of their main websites that provide information and service to the public. This check is required once every five years, and the first check must be performed no later than November 2023. Of the ten bodies that did not perform an accessibility check, four reported that their websites have been accessible for at least five years.

- **Appointing an Accessibility Coordinator –** out of the 23 government bodies that responded to the survey, three (13%) indicated that they did not appoint an accessibility coordinator – the Ministry of Interior, the Ministry of Religious Services, and the Central Election Committee. The appointment of an accessibility coordinator is required by law from a body that provides a service to the public and employs over 25 employees, for the promotion of its activity and to address public inquiries.

- **State Comptroller's Office Accessibility Checks –** the State Comptroller's Office checks of 15 websites of 14 government bodies – the National Insurance Institute, the Ministry of Religious Services, the Courts Administration (the Net Ha'Mishpat website, and the Supreme Court website checked), the Central Election Committee, the Israel Knesset, the Israel Police, the Ministry of Defense – the Rehabilitation of Disabled Veterans Department, the Ministry of Health – the Call Health website, the Ministry of Interior, the IDF – the Meitav Unit website, the Population, and Immigration Authority, the Enforcement and Collection Authority, the Nature and Parks Authority and the Employment Service – raised in each of them items that were not accessible as required by law for persons with various disabilities. As part of the checks of all these websites, documents, online forms, or visual elements were found not as accessible as required.

## The Rate of Proper and Defective Accessibility of Items in each of the 15 Websites Examined *


* As part of the check, a limited number of items were sampled and examined at each website. The rates shown in the diagrams do not always equal 100% as they have been rounded.

**Accessibility Checking of Service Pages –** in checking the accessibility of the service processes of the 16 most common online service pages, providing information about a digital service on the websites and sometimes even links to online forms to receive the service, at least two items were found not accessible as required by law. Below is a breakdown of the service pages that were checked:

| The Service Examined | The Government Body |
|---|---|
| Producing a land registration extract from the land registries | Ministry of Justice, Land Registry and Settlement of Rights Authority |
| Payment of traffic fines | Israel Police |
| Declaration of a passenger entering Israel before a flight (for the covid-19 period) | Ministry of Health |
| Car registration renewal | Ministry of Transport and Road Safety |
| Disabled parking tag | Ministry of Transport and Road Safety |
| Issuing a driver's license | Ministry of Transport and Road Safety |
| Driving license renewal | Ministry of Transport and Road Safety |
| Transferring ownership of vehicles | Ministry of Transport and Road Safety |
| Passport application | Population and Immigration Authority |
| Application for an ID card | Population and Immigration Authority |
| Information on withholding tax certificates and bookkeeping | Israel Tax Authority |
| Checking the processing status of an application for a job grant | Israel Tax Authority |
| Applying for a job grant | Israel Tax Authority |
| Tax adjustment online | Israel Tax Authority |
| Real estate information | Israel Tax Authority |
| My ILA (information from the Israel Land Authority) | Israel Lands Authority |

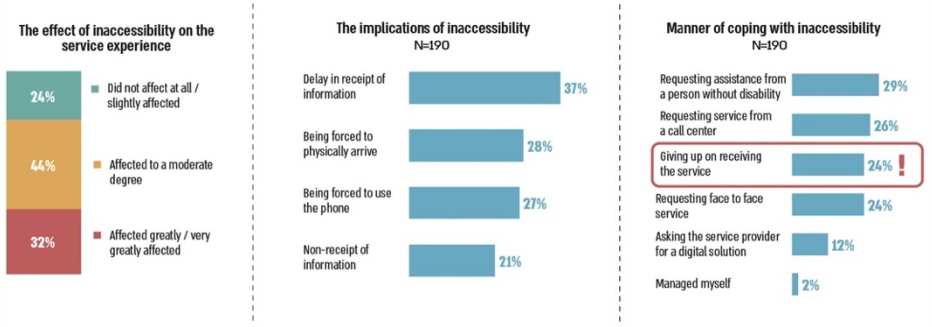
## Public Participation Among Persons with Disabilities

**Preference for Traditional Service Channels –** in the State Comptroller's Office public participation survey among persons with various disabilities, a representative sample of persons with disabilities who use the Internet, it was raised that a significant rate of the respondents – 44% – prefer to physically come to the public reception bureaus

to consume the government services or use the phone service and not through the digital channels.

**The Impact of Accessibility Problems in Digital Service Channels –** 39% of the respondents to the public participation survey stated that they had encountered items that were not accessible as required on government bodies' websites or apps. Below is the diagram of how these respondents cope with accessibility difficulties on the digital channels and the implications for their service experience.

**The Implications of Accessibility Difficulties in Digital Service Channels and Their Coping with them***




* The sum of the percentages in the sections "Manner of coping with inaccessibility" and "Implications of inaccessibility" exceeds 100% because each respondent could indicate more than one possible answer.

**Supervision by the Commission for Equal Rights of Persons with Disabilities –** the Commission for Equal Rights of Persons with Disabilities checks in 2019–2021 found accessibility deficiencies in the websites of 14 government bodies. The Commission alerted each body of the deficiencies it found but did not follow up on rectifying them in five bodies (36%).

**Accessibility Instructions for Healthcare Providers –** until the audit completion, November 2022, no regulations was imposed on healthcare providers, (including health maintenance organizations and hospitals) that provide service to the general public in Israel, to make their websites or apps accessible to persons with disabilities. Without a legal requirement, it is impossible to force health service providers to make accessibility adjustments on the websites.

**Measuring the Quality of the Digital Government Service for Persons with Disabilities –** even though about 17% of the population in Israel are persons with disabilities, the Improvement of Government Service to the Public Unit in the National

Digital Agency did not measure the quality of the government digital service provided to the public regarding accessibility to persons with disabilities. Therefore, no relavant information can be found in the annual reports it published.

**Consolidated Infrastructure for the Government Bodies Websites –** the National Digital Agency provided the government bodies with a consolidated infrastructure for the websites that provide information and services to the public. In this infrastructure, some accessibility adaptations that must be provided in the websites for persons with disabilities, such as connecting with screen reading software and contrast at the required level, have been implemented.

## Key Recommendations

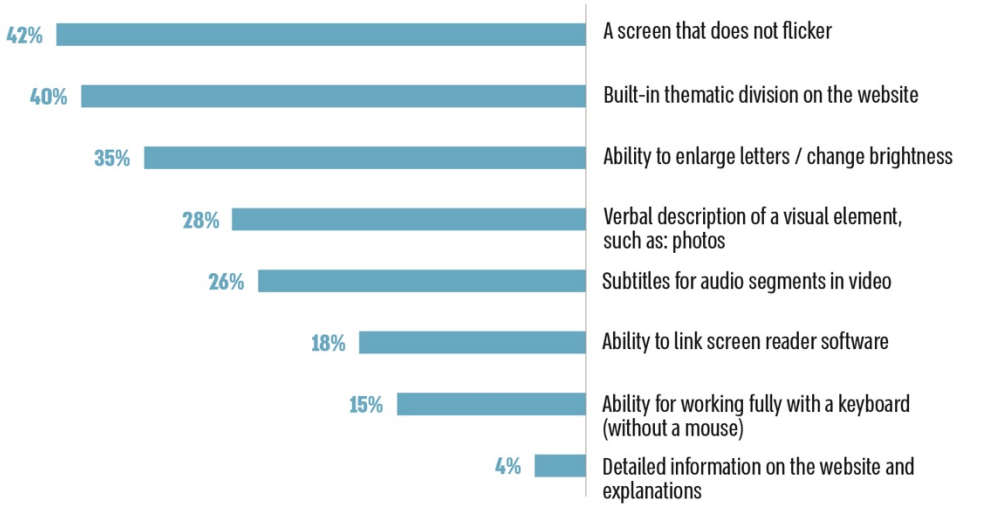
- Government bodies should systematically make accessible to persons with disabilities all the content and public services on their websites. In this framework, among other things, every document prepared since October 2017 and uploaded to the website and all the online forms used to receive service should be accessible. Government bodies should also provide alternative text for visual items and prepare subtitles for videos and audio segments containing speech.
- Government bodies should periodically check every website intended for public service to ensure that all the items requiring accessibility have indeed been made accessible generally and to all types of disabilities. If the check raises deficiencies in the accessibility or items that were not made accessible as required, the deficiencies should be rectified as soon as possible.
- Each of the bodies whose websites were checked by the State Comptroller's Office for the accessibility of items should rectify the deficiencies found during the check – the National Insurance Institute, the Ministry of Religious Services, the Courts Administration (the Net Ha'Mishpat website and the Supreme Court website), the Central Election Committee, the Israel Knesset, the Israel Police, the Ministry of Defense (the Rehabilitation of Disabled Veterans Department website), the Ministry of Health (the Call Health website website), the Ministry of Interior, the IDF (the Meitav Unit website), the Population and Immigration Authority, the Enforcement and Collection Authority, the Nature and Parks Authority and the Employment Service.
- Regarding digital service pages, the bodies whose service pages have been inspected by the State Comptroller's Office, whether their service pages are under the purview of the National Digital Agency or if their service pages direct to computer systems under their responsibility, should make the necessary rectifications and regulate the accessibility of

these pages so that persons with disabilities will be able to receive service on the websites like the rest of the public, as required by law. They should do it themselves or in collaboration with the National Digital Agency.

- It is recommended that the Commission for Equal Rights of Persons with Disabilities periodically monitor, ensureing full compliance with the requirements of the law regarding the accessibility of government bodies websites to persons with disabilities. It is further recommended that the Commission annually survey persons with various types disabilities and obtain information about the accessibility deficiencies they encounter when consuming government services through digital channels. This will help it focus the accessibility checks it does on government bodies.

- It is appropriate that the Ministry of Health establish provisions to regulate the accessibility of internet content and services provided by health services to the public.

**The Findings of the State Comptroller's Office Public Participation Procedure Among a Representative Sample of Persons with Disabilities – the Rate of Respondents Requiring a Certain Type of Accessibility on the Internet, According to the Types of Accessibility**



# Summary

Government bodies provide the public with many services through websites and apps. This has advantages both for the bodies themselves in terms of efficiency and economy and for the citizen, to whom the service is generally available anywhere and at any time, without waiting for his turn at the public reception bureaus or on the phone. Apart from the advantages of using digital service channels, they become essential in times of crisis, such as a pandemic or war, because at such times, they may become the main channels through which the public can receive information and service. After the outbreak of the covid-19 crisis in 2020 and its aftermath, the need for digital communication channels to connect the public and government bodies increased, and the government accelerated the development of its digital services. In 2022, as part of this audit, the State Comptroller's Office checked the accessibility of the digital services of government bodies to persons with disabilities of various types, 17% of the population in Israel. The findings indicate that the government bodies' websites have thus far been made partially accessible. The lack or partial accessibility of information and service make it difficult and even prevent a person with a disability from consuming the government service on the digital channel in an independent and dignified manner. The right to receive an accessible service from a government body, including through digital channels, is essential for every person, particularly for persons with disabilities, as some have frequent interactions with government bodies due to the need to exhaust rights arising from their disabilities. This right is anchored in Israeli law and is even presented in the International Convention on the Rights of Persons with Disabilities, which the State of Israel signed in March 2007 and ratified in September 2012.

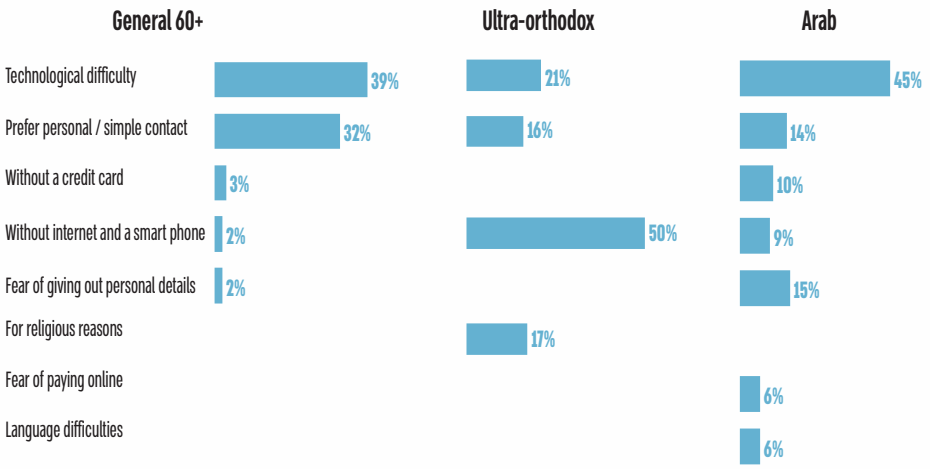
In this report, in-principle recommendations were given to all government bodies to perform accessibility checks in their digital services and rectify deficiencies. Recommendations were also given to the regulating bodies – the Commission for Equal Rights of Persons with Disabilities in the Ministry of Justice and the National Digital Agency – to promote digital accessibility of government services. Individual findings found as part of the State Comptroller check on government bodies websites and their service pages were transferred during the audit to each of the bodies so they could as soon as possible rectify them. The more the government bodies use the audit findings to rectify deficiencies found and address the digital service channels' accessibility, the more they will be able to improve the service they provide to persons with disabilities, which may motivate many more of them to use these channels and benefit from the advantages inherent therein.

# Part Two: The Government's Response to Non-Users of Digital Media in the Digital Age

## Key Findings

- **Three Population Groups that Seldom Consume Online Government Services –** according to the CBS data for 2021, in Israel, there were about 5.9 million people aged 20 and over. Of these, nearly 3 million people belong to three population groups that rarely, compared to the general public in Israel, consume online government services – people over 60, the ultra-orthodox society, and the Arab society. These groups comprise about a third of the total population in Israel (which in that year was about 9.5 million people) and almost half of the adult population. The findings of the State Comptroller's Office survey among people from these three groups indicate that they face barriers that make it challenging to use these channels, and therefore, they prefer not to use them. These barriers originate from the lack of appropriate means or technological difficulties in operating the service on the digital channel. Under these circumstances, the traditional channels (public reception bureaus, phone, and mail) are the only alternatives for them to receive the service.

## The Reasons for Not Preferring Digital Channels for Receiving Government Service




Findings of a phone survey conducted by the State Comptroller's Office.

- **Need for Digital Means and a Credit Card in Traditional (non-digital) Service Channels –** 31% of the respondents to the State Comptroller phone survey among people who rarely consume services on the internet or refrain from it, stated that they encountered cases where they wished to receive a government service through a traditional channel but did not receive a response because they were required to use means they did not possess, such as a smartphone, e-mail or credit card. About 13% of the respondents who stated that they encountered difficulties consuming services through the traditional channels do not have a smartphone, which requires them to receive a password for identification purposes. This means is required in the phone service channel. 9% stated that when they asked to receive service at the bureau, they had to make an online appointment, placing a barrier in front of them. Furthermore, 4% of the respondents stated that they did not have a credit card and, therefore, asked to pay at a register using cash but were refused.

- **Response Exclusively Through the Digital Service Channel –** of the 520 respondents to the State Comptroller's Office online survey, among persons with disabilities who use the Internet, 199 respondents (38%) stated that they encountered cases where it was not possible to receive service from government bodies except through digital means. That is, they could not consume the service at a public reception bureau or through the phone service. It should be noted that according to the respondents' answers, sometimes the referral to the digital service as an exclusive channel for receiving the service was already done at the initial stage, where they wished

to make an appointment to receive the service and were directed to the digital service that was the only way to make the appointment.

- **Digital Service Stations at Public Reception Centers –** digital service stations at public reception bureaus of government bodies can help citizens who do not have a means of connecting to the internet to consume information and services digitally. However, in the State Comptroller's Office survey among 23 government bodies, only six bodies indicated that they had placed such stations in their public reception bureaus.

- **Making the Government Digital Service Accessible to the Arab Culture and Language –** to make the government service accessible to the Arab culture and language, in October 2021, the government decided (Resolution 550) that at least 50% of the relevant digital government content and services will be linguistically and culturally accessible to the Arab population by the end of 2025. The audit raised that as of August 2022, the Arabic translation of the online forms in the ten most common government services (defined by the National Digital Agency) has not been completed.

# Key Recommendations

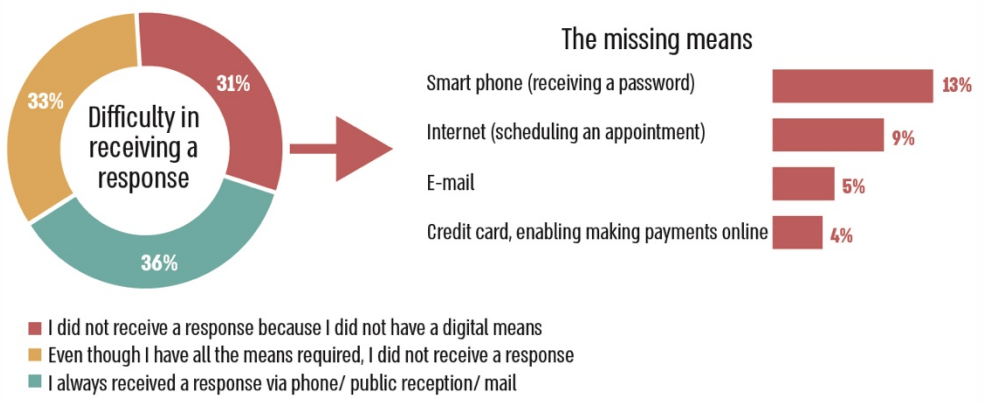
- It is recommended that the National Digital Agency and the government bodies study the findings of the State Comptroller's Office public participation surveys, analyze the barriers or reasons for the relatively low use of the digital channel among the ultra-Orthodox and Arab population and those aged 60 and over, for the consumption of government services, and consider improving the government service for such large groups in the Israeli public, which together make up about a third of the population. Concurrently with the development of digital services, making them optimally accessible to the general public, the government bodies should continue providing a complete response through traditional channels for those who prefer or are forced to use them.

- Government bodies should provide service through traditional channels – public reception bureaus, phone, and mail – without making it conditional on using digital means, such as e-mail and smartphones. Likewise, a person who wishes to pay a government fee at the register in a public reception bureau should be able to do so without making it conditional on using a credit card since some people do not use this means.

- It is recommended that the National Digital Agency, in cooperation with each government body that provides digital services to the public and has not yet placed digital service stations in their public reception bureaus consider their placement. Thus, making the information and services in digital channels accessible to the general public, including people who have difficulty using technology or lack the appropriate means.

It is appropriate that the National Digital Agency and the government bodies complete the translation into Arabic and publish service pages currently on the consolidated government website not published in Arabic. Thus increasing the government services accessibility to the Arab-speaking population according to the government's resolution purpose.

**The Respondents Rate who Encountered Difficulty in Receiving Service from Government Bodies by Phone or at a Public Reception Bureau due to a lack of Digital Means or a Credit Card**




Findings of a phone survey conducted by the State Comptroller's Office.

# Summary

There are three main population groups that, compared to the general population, rarely use the Internet in general and for the consumption of government services in particular: those aged 60 and over, as well as those aged 20 from the ultra-Orthodox Jewish society and the Arab community. These groups together are over 3 million citizens – about a third of the population in Israel and about half of its adult population. The State Comptroller's Office conducted a public participation phone survey. 300 people who belong to these three groups who participated in the survey stated that they prefer not to use the digital government service channels and noted the barriers that make it difficult for them to use these channels. The main barriers are low digital literacy and not having a means of connecting to the internet. These barriers, as well as other barriers noted, are also related to personal preferences and cultural and social reasons, such as refraining from possessing a smartphone or a computer connected to the internet among people from ultra-orthodox communities and the relatively limited use of credit cards among the Arab society.

In this current era, characterized by the transition from traditional service to digital service, government bodies should address the barriers that prevent certain population groups from reducing the gap to the digital age. Actions to increase digital literacy among these three groups have been carried out in recent years by the National Digital Agency, following government resolutions, and these should continue even more vigorously. Placing digital service stations in the public reception bureaus of government bodies, with attendants who will assist their users, can help populations that do not own digital means and people with low digital literacy to consume government services in this way. Along with such actions, the government bodies should maintain their traditional service channels and even improve them to enable people who need them to consume the services and exercise their rights. This is also necessary to minimize the gap between them and those who use a government service on the digital channel. This is of significant importance as the socio-economic status of people from these population groups is usually lower than that of the general population. Therefore, they are more in need of the service provided by the government bodies. In this context, it is recommended not to stipulate the receipt of the service in a traditional service channel on the need to use a digital means (or a credit card to pay at the register) since some of the people who turn to the traditional channels do not use these means. They should not be denied service but rather be assisted in receiving the service and help.

State Comptroller's Report – Cyber and Information Systems | May 2023

The Ministry of Interior

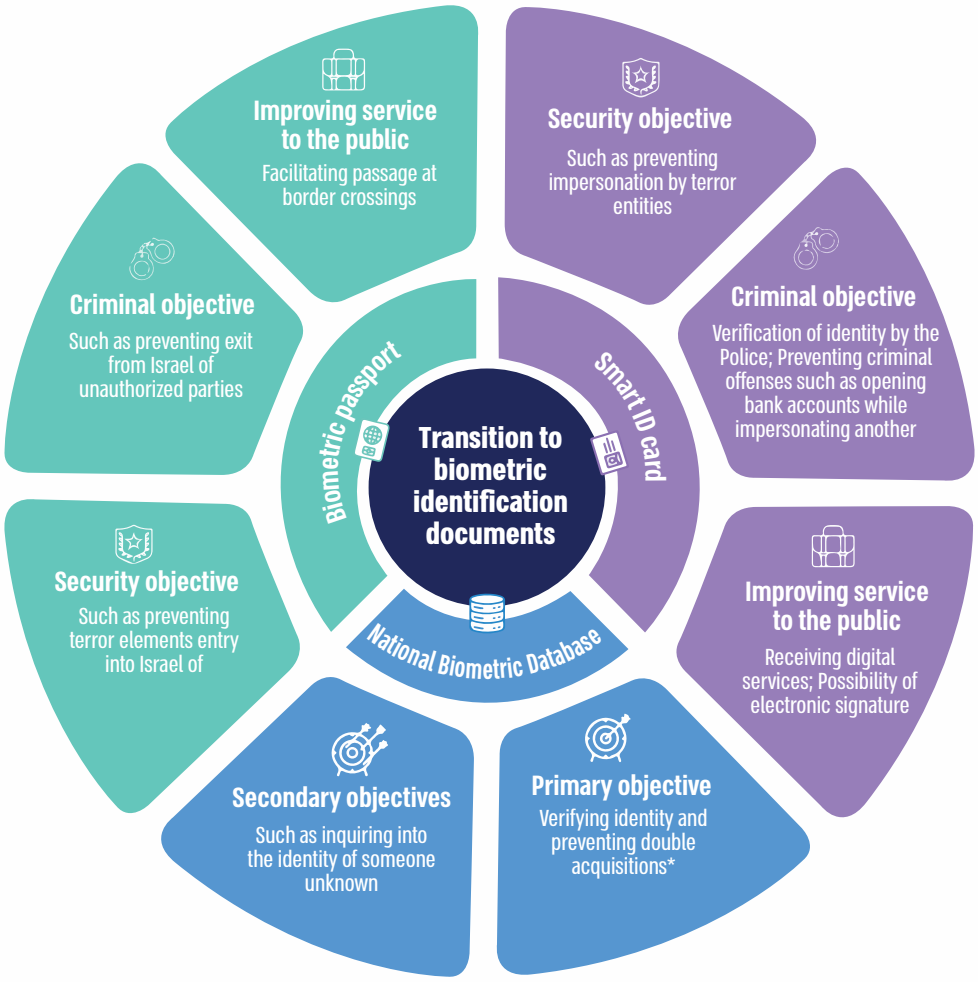
# Use of Biometric Identification Documents – ID Cards and Passports

# Use of Biometric Identification Documents – ID Cards and Passports

## Background

Identification documents of a state's residents and foreigners entering it, such as ID cards and passports, are used for managing the state and maintaining its security. For years, the identification documents issued in Israel were considered easy to forge (old-type ID cards or passports). As a result, the Ministry of Interior promoted a project to issue identification documents that would be difficult to forge, improve the reliability of identification and enable the provision of advanced services to the public. In 2008, the government resolved to replace the identification documents with smart identification documents through biometric identification and to keep the biometric information in a national biometric database. The objectives of the transition to biometric identification documents are presented in the diagram below:

## The Objectives of the Transition to Biometric Identification Documents and its Components




* Double acquisition – where a person impersonates another and receives an identification document indicating the name of another, but where the biometric characteristics included therein are those of the impersonator. This way, a person can have several identities.

## Key Figures

**NIS 935 million**

the transition cost to issuing biometric identification documents 2009–2021

**45%**

of the ID card holders (about 3.2 million residents) still hold an old-type ID card as of July 2022

**37%**

of the passport holders (about 2.9 million residents) still hold old-type passports, which are easy to forge, as of July 2022

**400**

attempts to enter the country using forged identification documents through border crossings under the purview of the Crossing Points Authority in the first half of 2022

**less than 1%**

of the residents who entered the National Identification System used the smart ID card to receive government digital services remotely

**92%**

of the residents who hold smart ID cards (about 3.5 million residents) have a card whose use requires a card reader, which is a barrier to the use thereof

**70%**

of the 3,834 residents who made three or more reports on the loss or theft of a smart ID card, have a criminal or police record

**30%**

of the Israelis who pass through the automatic checkpoints at Ben Gurion Airport, which are designed for biometric passports, pass through them using an old-type passport

**17%**

of the passports issued in the first half of 2022 are old-type passports

**65,000**

temporary passports (of the old type) were issued at the temporary passport center from the end of May 2022 to the end of August 2022

**6 weeks**

the time in which the Population Authority undertook to send residents their passports was extended from three weeks to six weeks

**3.6 million**

residents have an ID whose validity is expected to expire in 2023–2024, expected to come to the Population Authority bureaus to issue a new ID card

| millions | millions | less than 1% |
|---|---|---|
| of Israeli residents' photos are stored in the "Aviv" system (the system in which the population registry is managed) | of Israeli residents' and foreigners' photos are stored in the "Rotem" system (the Border Control's computerized system) | of those applying for biometric identification documents in the months of August – October 2022 requested that their fingerprints be stored in the national biometric database (197 out of 276,000 residents) |

## Audit Actions

From April to October 2022, the State Comptroller's Office audited the transition to biometric identification documents and their use, including the transition to smart ID cards and the barriers to their use; The transition to a biometric passport and the passage of Israeli residents and foreigners at Ben Gurion Airport; The Population Authority's coping with the demand increase for biometric identification documents and the existence of biometric facial image databases at the Population Authority. The examination was conducted at the Population and Immigration Authority (Population Authority), the Ministry of Interior, the National Biometric Database Authority, and the Biometric Applications Unit in the National Cyber Directorate. Completion examinations were carried out at the Ministry of Foreign Affairs, the Israel Police, the National Cyber Directorate (the Cyber Directorate), the Israel Security Agency (ISA), the Ministry of Justice, including at the Privacy Protection Authority, the Crossing Points Authority at the Ministry of Defense, at the National Security Council (the Prime Minister's Office), in the National Digital Agency, the Bank of Israel, the Institute for Intelligence and Special Operations (Mossad) and the Airports Authority. Furthermore, visits were conducted at the Ben Gurion Airport and the Qalandiya border crossing, as well as the production plants, for the issue of biometric identification documents.

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

# Key Findings

- **The Transition to the Smart ID Card –** even though the transition to smart ID cards began a decade ago, in June 2013, for residents expressing a desire for them, and in an obligatory manner for all residents in July 2017, and although NIS 430 million have been invested thus far in issuing them, as of July 2022, about 45% of those holding ID cards (about 3.2 million residents) still hold the old type of card, which is easier to forge. The continued use of these cards has criminal and security implications. Thus, in the first half of 2022, at the border crossings under the purview of the Crossing Points Authority, about 400 attempts to enter the country using forged documents were recorded.

- **Correlation Between Repeated Requests to Issue a Smart ID Card and Involvement in Crime –** a correlation was found between the number of times citizens reported the loss or theft of smart ID cards and asked to issue new cards and the criminal or police record of these citizens. Since the issuance of smart ID cards began in June 2013–3,834 residents have reported the loss or theft of a smart ID card three or more times, and 70% of them have a police or criminal record. Among those who submitted such a request eight times or more, this rate was 100%.

- **The Use Scope of a Smart ID Card to Receive Government Services –** due to barriers, including the need for a card reader and remembering the password, the use of the smart ID card for identity verification and receiving digital government services is extremely limited and almost negligible – less than one percent of residents used it for receiving services in the National Identification System. This, despite the identification using it, is more secure. Consequently, one of the objectives of the transition to a smart ID card – providing advanced services to the public while using it – was not achieved.

- **Biometric Identity Verification Using the Smart ID Card –** as of September 2022, the Population Authority is the only body among the enforcement entities and government bodies authorized by law[1] to use the biometric layer of the ID card to verify a person's identity (1:1)[2]. Even it does it in a limited way, only when the holder of the smart ID card physically arrives to receive service at the Authority's office. It was raised that the Police, and the government ministries, do not use the biometric layer of the smart ID card.

- **Barriers Hindering Biometric Identify Using the Smart ID Card –** due to legal and technological barriers concerning access control to the facial image in the smart ID card chip, the possibility of using it to perform biometric identification verification is

1 The Inclusion of Means of Biometric Identification and Biometric Identification Data in Identification Documents and in a Database Law, 2009 (the Inclusion of Biometric Means of Identification Law).

2 Comparison of the means of biometric identification taken with the previously saved sample.

limited. As of July 2022, about 3.8 million residents held a smart ID card. Since it is impossible to retroactively change the access control in the cards that have already been issued – even when these barriers are removed, these residents will not be able to use them to receive a significant part of the services that require biometric identity verification. Moreover, 580,000 smart ID cards have embedded in them a chip with a small memory capacity, and their holders will not be able to use the ID card to receive services requiring biometric identity verification.

- **A Certified Electronic Signature on the Smart ID Card –** at the audit completion, about 13 years after it was stipulated in the law that the smart ID card would enable a resident wishing to do so to include a certified electronic signature, this option is not realized, since the Population Authority has not completed the preparation required to comply with the Privacy Protection Authority's requirements (Certification Authority Registrar). As a result, residents who are required to perform actions that require a certified electronic signature are forced to pay commercial parties for this service or alternatively go to a service bureau to perform actions requiring a signature.

- **The Transition to a Biometric Passport –** at the audit completion, about a decade after the issuance of biometric passports began (in June 2013) for residents expressing a desire for them, and in an obligatory manner for all residents in July 2017, about 2.9 million residents, about 37% of all passport holders, still hold old-type passports that are easy to forge.

- **The Passage of Israelis at the Ben Gurion Airport**

  - From the Population Authority documents and visits, observations, and attempted passing through border points conducted by representatives of the State Comptroller's Office, gaps were found in the conduct of the Population Authority in implementing a procedure it established to block a breach enabling foreign and Israeli crime and terror elements to enter and leave the country. This is a genuine breach of border control.

  - The audit raised that this was a risk that had materialized, and the report presented several examples of incidents where various people entered or left the country, taking advantage of the said vulnerability in border control. It should be noted that these examples do not represent the extent of the exploitation of this vulnerability since these are only instances that have been found. However, these incidents and the attempted crossing of the representatives of the State Comptroller's Office while taking advantage of the said vulnerability (an attempt that succeeded) are adequate to illustrate the risk and clarify that it is genuine and is well-known to the Population Authority. Moreover, these incidents raise the concern that this vulnerability is also known to those who seek to abuse it. It is impossible to know how many such instances have occurred thus far, what is the identity of the people who left the

country or entered it, and why they crossed while taking advantage of this vulnerability.

- **The Entry of Foreigners into Israel –** by the analysis of Border Control data and the representatives of the State Comptroller's Office observations, as well as a series of incidents in which foreigners entered Israel without being inspected as required, the working method at the Border Control regarding foreigners at Ben Gurion Airport is not consistent with the guidelines of the Border Control Administration and enables the entry of foreigners, without verification that their entry into the country should be approved. This report, therefore, exposes actual breaches in the entry of foreigners through Ben Gurion Airport.

- **Continued Issuance of Old-Type Passports, Easy to Forge –** from the end of the trial in June 2017 to the end of June 2022, half a million old-type passports were issued, about 10% of all passports issued during this period; In the first half of 2022, there was an increase in the number of old-type passports issued, and their rate was about 17%. Continuing to issue old-type passports (temporary passports and passports issued by Israeli embassies abroad) is not in line with the objectives of the transition to biometric documentation, and it even increases the risk that unauthorized people, including criminal and terrorist elements, will attempt to leave the country and enter it using a forged Israeli passport.

- **Issuing Passports at Israeli Embassies Abroad –** the project outline for issuing biometric passports by Israeli embassies abroad was formulated in 2015. Still, for seven years, until 2022, their issuance did not begin, and tens of thousands of old-type passports, which are easy to forge, are issued every year.

- **The Population Authority's Preparation for the Crowded Queues Following the Covid-19 Pandemic –** during the Covid-19 pandemic, a backlog accumulated in the issuance of about one million passports compared to the volume of issuance in 2019: at the end of 2019, before the outbreak of the Covid-19 pandemic, the percentage of Israelis who held a valid passport was more than 75%, while at the end of May 2022, the rate was only about 63%. This resulted in the formation of a heavy burden on the Population Authority, including difficulty in making appointments. It should be noted that the measures taken by the Population Authority to cope with the rising demand for passports in the post Covid-19 period, including opening a center for issuing temporary passports, expanding the hours of operation of the passport manufacturing production plant and bureaus, and recruiting personnel for this purpose. However, some of the measures have consequences manifested in a delay in the completion of the transition to the national biometric documentation (postponing the expiration date of the old-type ID cards by two years, increasing the scope of temporary passports, and extending their validity). Some have consequences for the Authority's actions (such as diverting personnel and reducing the Authority's enforcement actions).

- **Time Extension for Issuing Passports –** it was raised that given the increase in demand for passports in the post Covid-19 period, the time the Population Authority undertook to send the passport was extended from three weeks to six weeks. Moreover, the Population Authority's passport production plant is equipped with outdated printers for issuing biometric passports, and the production dependent thereon does not meet the demand for biometric passports in an increase in demand. In November 2018, the Population Authority began procedures to examine the procurement of advanced printers to increase the number of passports produced and meet the population's demand for their supply. It was found that four years later (as of September 2022), the Population Authority still has not completed the process of replacing the printers in the passport-issuing production plant with advanced printers. Furthermore, the Authority does not have printers as backups to print biometric passports in the event of the shutdown of the issuing production plant. I.e., it will be impossible to issue biometric passports if the issuing production plant is shut down.

- **The Population Authority's Preparation for Future Crowded Queues at the Bureaus –** in the next two years (2023–2024), the ID cards of 3.6 million residents are expected to expire (old-type ID cards and biometric ID cards whose validity is expected to expire). The holders of these cards are expected to come to the Population Authority bureaus to have new identification documents issued. This is in addition to the regular inquiries to the Authority's bureaus. That is, it is an average monthly increase of about 150,000 inquiries over the average inquiries per month in 2019 which was about 200,000 inquiries (an average monthly increase of about 75%). Even if there is some overlap between the rate of residents who regularly come to the bureaus and those who are expected to attend the bureaus in the next two years to issue new ID cards, this is a considerable increase, requiring preparation. It was raised that the response formulated by the Authority to the burden of inquiries expected in its bureaus in the coming years – placing self-service stations – will provide a partial response: the stations will not respond to the 3.9 million residents who, as of September 2022, do not have biometric identification documents (biometric passport or smart ID card); Furthermore, at this stage, the stations are not planned for providing service to minors with biometric identification documents.

- **The Population Authority's Facial Image Databases –** alongside the national biometric database, the Population Authority has facial image databases of millions of residents in its information systems. Due to technological developments, facial images are of biometric quality, and therefore the possession of the databases is not consistent with the provisions of the law. Furthermore, these databases' protection level is less than that of the national biometric database. As of October 2022, about three years after the Commissioner of Biometric Applications first alerted about this issue, the Authority has not formulated a solution.

- **Preparing for the Procurement of the Technological Means Required to the Transition to a Database Based on Facial Images Only –** for the National Biometric

Database Authority to be able to fulfill its role – prevention of identity fraud and double acquisition – it should be equipped with a biometric comparison system. In 2017, the law stipulated that upon the expiry of the temporary order[3], the biometric database would be based on facial images only, and the fingerprints in it would be deleted. Still, it was raised that the existing biometric comparison system is unsuitable for this purpose. Even though in 2020, the Head of the Cyber Directorate determined that there are technological means suitable for basing the database on facial images only, it was in December 2022 that the National Biometric Database Authority published the first stage of a tender for the purchase of a biometric comparison system suitable for this purpose. According to the Ministry of Interior, the system is expected to be integrated in the fourth quarter of 2024.

**Saving Fingerprints to Identify Victims of a Mass Casualty Incident –** alongside the stipulation in the law in 2017 that the national biometric database will be based on facial images and the fingerprints in it will be deleted starting in September 2020, the Ministers of Interior asked to examine whether it is necessary to save the fingerprints in the database to use them for a secondary purpose prescribed in the law – identification of victims in a mass casualty event. However, as of November 2022, about two years after the need to examine the secondary use of fingerprints was raised, the Ministry of Interior has not decided on the use of fingerprints, which as of December 2022, are still stored in the national biometric database.

**Updating the Operating Doctrine –** in 2008, the operating doctrine for the national biometric documentation project was formulated, assuming that it would be valid for about a decade. At the audit completion about 15 years later, it was raised that the Ministry of Interior had not updated it. This is despite far-reaching changes in fundamental aspects affecting the project, including the Widespread proliferation of facial images on social media; A significant improvement in the capabilities of facial recognition technology, including the use of algorithms based on artificial intelligence, Expansion of online services that require secure remote authentication; Allowing passage using biometric passports at automatic stations at border crossings; The existence of significant barriers to the use of smart ID cards; Amendment to the law stipulating that the national biometric database will include facial images only; And the keeping of biometric databases of facial images by the Population Authority.

**Measures to Leverage the Use of the Smart ID Card –** to try to leverage the use of the smart ID card and remove the barriers that make use thereof difficult, the Population Authority decided to switch to the second-generation ID card (the chip in which can be accessed via an NFC device and therefore a card reader is not required for use thereof). In addition, in collaboration with the Population Authority, the Biometric

3 At first it was determined that the temporary order would be in effect until May 2022, and later it was extended until June 2023.

Applications Unit developed a prototype known as "Shomer Zahav," which enables verification of the resident's identity using the smart ID card. The development is intended to enable the entities authorized by law to perform biometric identity verification of a person offline against their certificate (such as at self-service stations – "kiosks").

**Supervision of the Implementation of the Provisions of the Inclusion of Biometric Means of Identification Law –** the Commissioner of Biometric Applications is established by the law as a supervisory body for implementing its provisions. The supervision carried out by the Commissioner of Biometric Applications raised gaps in several topics, and these gaps were presented to the public in periodic reports published by the Commissioner, leading to the promotion of this vital project.

# Key Recommendations

- It is recommended that the Population Authority encourage the public to replace the old-type identification documents in their possession even before they expire and that it clarifies to the public the inherent risk of continuing to use them as they are easy to forge.
- The Population Authority, in cooperation with the National Digital Agency, the Ministry of Justice, and the Commissioner of Biometric Applications at the National Cyber Directorate, should urgently remove the legal and technological barriers that make using smart ID cards difficult, primarily the strict access control. Removing the barriers and increasing the number of bodies authorized to perform biometric identity verification against the smart ID card may improve the identification processes considerably and enable to realize the potential inherent therein.
- The Population Authority should implement its procedure to resolve the vulnerability at the border control presented in the report regarding crossing using Israeli passports. However, given the warning from some of the professional elements of the Authority cautioning that even the solution in the procedure does not provide a sufficient response to the risk, the Authority should ensure without delay that the border control at Ben Gurion Airport is effective and mitigates the risks involved in the passage through the border crossings, against the considerations of congestion and queues, in particular, public security considerations and the need to prevent the entry and exit of unauthorized people.
- The Population Authority, in cooperation with the Israel Security Agency, should quickly rectify the situation described in the report, which allows unauthorized foreigners to enter Israel at the Ben Gurion Airport, and to ensure that the Border Control process achieves its goals. It is recommended that the Authority formulate an updated procedure for border control at the Ben Gurion Airport regarding foreigners passing through it, anchor the procedure that will be established in its procedures, and ensure that all the parties comply

with it. It is also recommended that the Population Authority audit the activities of the Border Control Administration to ensure its operation under the established rules.

- Given the role of the Israel Security Agency in protecting against terrorist threats, given the risk posed by the entry of foreign terrorist elements into the country at the border crossings, and given the audit findings about vulnerabilities in the border control at Ben Gurion Airport, it is recommended that following an up-to-date risk analysis, ISA will examine, in consultation with the Population Authority, the need to amend legislation so that the Border Control Administration is included in the First Schedule to the Regulation of Security in Public Bodies Law, 1998, and so that it will be guided by the ISA[4]. This is while considering the entirety of security risks at the national level.

- It is recommended that the Population Authority formulate a detailed work plan to cope with burdens on the Authority's bureaus based on data regarding the expected inquiries (including 3.6 million applications for smart ID cards to replace cards whose validity is expected to expire in the next two years) compared to the processing capabilities of the bureaus and ensure that the planned solutions should respond to the public's inquiries, at a satisfactory level of service. This includes a recommendation that the Population Authority send a notice to the holders of identification documents whose validity is expected to expire so that they can make an appointment at the bureaus ahead of time; And that it will unify the renewal dates of the two biometric identification documents – ID card and passport. This is to ease future burdens and improve the service to the public so that they are required to come only once to renew their identification documents.

- To ensure the response to the demand for issuing biometric passports at peak times and to improve the service to the public, it is recommended that the Population Authority complete the purchase of the advanced printers for the biometric passport production plant and integrate the use thereof. It is also recommended that the Population Authority place printers as backups to ensure functional continuity if the issuing production plant is shut down.

- The Population Authority, with the assistance of the Ministry of Justice, should regulate the possession of its biometric facial image databases from the legal aspect, or it should delete the databases while addressing the need raised by the Authority to identify the service applicants, for example by forming an outline enabling reliance on the information stored in the national biometric database. This is subject to maintaining privacy protection and information security. Furthermore, the Population Authority should protect the databases above in its possession according to their degree of sensitivity.

- Since the law stipulates that the national biometric database will be based on facial images only, the fingerprints in the database are "excess information." Once the Ministry of Interior reaches a decision regarding the need to continue keeping the fingerprints in the biometric

4 This is in addition to the guidance of the Population Authority by the Cyber Directorate, stipulated in the Fifth Schedule to the Regulation of Security in Public Bodies Law, 1998.

database to identify victims in a mass casualty event, it should consult with all relevant parties regarding the national biometric database and consider the following aspects: can the fingerprints be left in the database for secondary use only, once it was determined that the fingerprints are not necessary to achieve the main objective of the law – preventing impersonation and double acquisition; What is the added value of the use of the fingerprints in the database over the use of the facial images stored therein; And in particular considering that these are fingerprints of only two digits, taken in a specific position, which may affect the ability to use them (straight and not rolled position); Since the amendment of the provisions of the law (in July 2022), less than one percent of applicants wishing to issue biometric identification documents, requested that their fingerprints be kept in the database (in the months of August-October 2022, the fingerprints of 197 residents out of approximately 276,000 residents were transferred to the database for their storing); And whether fingerprints are collected for this in other places around the world. Moreover, given the public sensitivity concerning the very existence of the national biometric database, it is recommended that the Ministry of Interior's decision and the legal and professional considerations underlying it be made public.

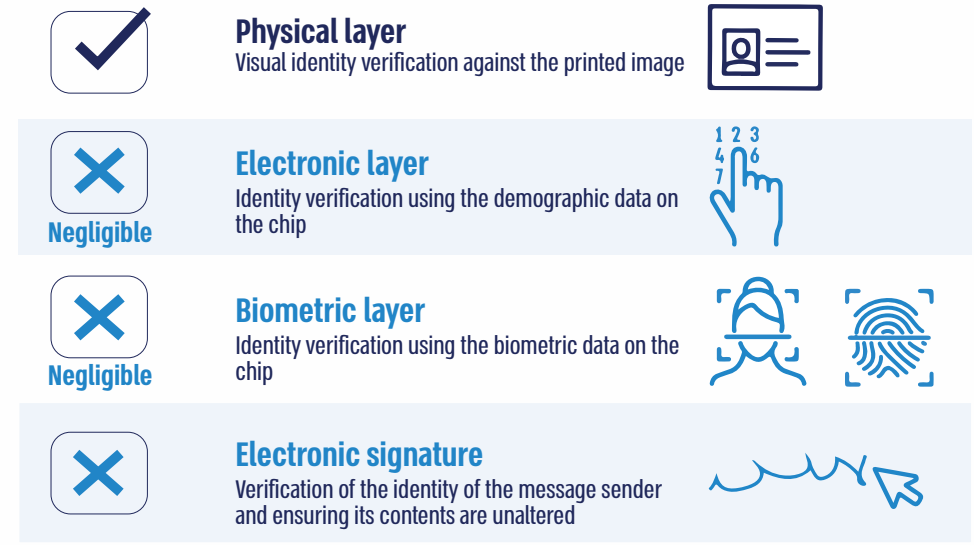
It is recommended that the Ministry of Interior, including the National Biometric Database Authority, ensure the transition to the biometric comparison system that will enable the database to be based on facial images only as soon as possible. It is also recommended that, if necessary, the Ministry of Interior and the Authority initiate an appeal ahead of time to the Joint Knesset Committee[5] to request another extension of the temporary provision. The need to promote the necessary actions is highlighted given the experience regarding the existing biometric comparison system, where there were considerable delays in the tender process for its purchase and implementation – four years have passed from the date of the engagement until it became operational.

To the extent that the Ministry of Interior resolves to expand the powers of the National Biometric Database Authority, it is recommended to involve the Privacy Protection Authority, the National Cyber Directorate, and the Commissioner for Biometric Applications in the procedures for formulating the proposed government resolution and the legislative amendments. This ensures that the Authority's activity considers the need to maintain information security and privacy protection. It is also recommended that the expansion of the authority of the National Biometric Database Authority, to the extent as long as it is decided, be done under the supervision of the Commissioner for Biometric Applications, whose role is to supervise the implementation of the provisions of the law and lead the national policy on biometric applications and secure identification.

5 The Joint Knesset Committee of the Constitution, Law and Justice Committee, the Interior and Environmental Protection Committee and the Science Committee, pursuant to the Inclusion of Means of Biometric Identification and Biometric Identification Data in Identification Documents and in a Database Law (the Joint Knesset Committee).

The National Biometric Documentation Project concerns various entities, including the Population Authority (the Population Authority bureaus and the Border Control Administration), the National Biometric Database Authority, and the production plants issuing the biometric identification documents. It is recommended that the Ministry of Interior form an updated operating doctrine that will address all the aspects related to the national biometric documentation with the participation of all the parties involved in the process and the risks and vulnerabilities raised in this audit report.

## The Use of the Layers of the Smart ID Card for Identification



# Summary

Reliable identification documents are critical to a wide range of operations in the government and business sectors. About a decade before the audit completion, in 2013, a transition to biometric identification documents began in Israel to enable secure identification, including remotely. The biometric identification documents are supposed to replace the old type of identification documents, which are considered easy to forge, may be used by terrorists or criminal elements, and may also be used for illegal immigration purposes. The period of the Covid-19 pandemic, during which there was a considerable increase in the use of digital channels, also for receiving services from government branches, highlighted the importance of secure identification in cyberspace.

The findings of this report raised substantial deficiencies in several main areas: a significant delay in the transition to biometric national documentation and the lack of use thereof; The existence of breaches in the entry and exit of Israelis and foreigners through Ben Gurion Airport; Disparities in maintaining biometric data; And the difficulty in coping with the demand increase for issuing biometric identification documents.

The Population Authority stated, regarding the breaches in the passage of foreigners and Israeli residents at Ben Gurion Airport, that there was indeed no strict adherence at Ben Gurion Airport to follow the procedures, and several measures were decided upon for addressing the issue.

Given the importance of the audit findings, it is recommended that the Population Authority rectify the deficiencies raised in the report and that the Minister of Interior ensure that the deficiencies in the areas above are indeed rectified, including deficiencies in information security and data protection in coordination with the professional bodies entrusted with the matter: the Israel Security Agency, the Police and the National Cyber Directorate.

Recently, there have been far-reaching changes in the national biometric project, Including a considerable improvement in the technological capabilities of biometrics. The use of online services that require secure identification has significantly increased. Completing the transition to biometric national documentation while removing the legal and technological barriers that make use complex and adapting the project to the changes in recent years may leverage the use of biometric identification documents and is expected to bring considerable benefits in defense, the economy, and public service.

State Comptroller's Report – Cyber and Information Systems | May 2023

The Ministry of National Security – The Israel Prison Service

# Digital Technologies and Information and Cyber Protection in the Israel Prison Service

# Digital Technologies and Information and Cyber Protection in the Israel Prison Service

## Background

The Israel Prison Service (IPS) is the national correctional organization, a security body, part of the law enforcement system and subordinate to the Ministry of National Security. The IPS was established in 1949 and, in 2006, was recognized as the State of Israel's national correctional organization. The IPS holds about 14,000 criminal, security, and administrative prisoners and detainees (and another 5,200 prisoners and detainees in incarceration alternatives and under supervision, under IPS responsibility) to protect peace and public security. As of the beginning of 2022, the IPS manages 30 incarceration facilities nationwide (22 prisons and eight detention centers), divided into three command districts – North, Center, and South, and employs 9,200 people. Its annual budget for 2022 was NIS 4.6 billion.

The IPS faces many technological challenges, and to cope with them, it operates through its Technological Division dozens of computerized organizational systems: Operational core systems for prisoner management and intelligence; Medicine and rehabilitation; Personnel, training, and logistics; Diverse security systems installed in incarceration facilities to protect them; Information security and cyber protection systems; And computerized systems in infrastructure, including server farms and a backup site. In 2006–2014, the IPS promoted a project to develop an organizational ICT system (the "Kidma" Project), which failed and was discontinued after an investment of NIS 144 million NIS therein. Beginning in 2021, under the IPS Commissioner's leadership and the Technological Division's Head, the IPS started implementing a strategic move designed to lead to a technological leap in the IPS. This strategic move was expressed in the formulation of the multi-year "Kabarnit" plan (the "Kabarnit" Plan), and its implementation began at the beginning of 2022. This plan, according to the IPS, is intended to shape and lead the IPS' new path as a dominant, innovative, and sophisticated security organization, and among other things, to establish an advanced and innovative work environment for the staff while increasing the use of technology, digitization, and innovation.

## Key Figures

**13%**
the decrease rate in the scope of the IPS technological budget in 2018–2021, while the total IPS budget increased by 12% in those years, and the average technological budgets of government ministries increased by 25%

**NIS 0.5 billion**
the multi-year budgetary cost to implement the "Kabarnit" plan, of which NIS 400 million is a technological budget

**75%**
of the technological budget needed to realize the "Kabarnit" plan has not yet been budgeted (NIS 300 out of NIS 400 million)

**38%**
the actual budget realization rate for the technological projects in the "Kabarnit" plan, planned for 2022 (NIS 39 million out of NIS 104 million). For another 62% of the budget, purchase orders were issued but have not yet been completed

# Audit Actions

From March to December 2022, the State Comptroller's Office audited digital technologies and cyber protection in the IPS. The audit includes three tiers as follows:

1. The digital technologies and information systems at the IPS. Including the budget for technology and technological governance at the IPS.
2. Information security, information, and cyber Protection in the IPS.
3. The functional continuity of the IPS technological systems and its effects on the functioning of the prisons in the event of a disaster.

The audit was carried out at the IPS Commission and in various prisons. Completion examinations were carried out at the Ministry of National Security, the National Digital Agency at the Ministry of Economy and Industry, the National Cyber Directorate (NCD) at the Prime Minister's Office, the Budget Division at the Ministry of Finance, and the Israel Security Agency (ISA). The State Comptroller conducted resilience checks on the IPS systems, and the findings were sent to the relevant bodies. The State Comptroller's Office conducted previous audits on various aspects of the IPS activities: "Establishment of an Information System in the Prison Service – the Kidma Project,"; "The Medical System for the Treatment of Prisoners in the Prison Service"; "Criminal Arrests in Israel"; And "Rehabilitation of Prisoners in Israel." Their findings and recommendations were published in the above audit reports.

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

# Part A – Digital Technologies and Information Systems in the IPS

## Key Findings

- **Drawing Lessons from the Kidma Project –** in the eight years since the failure of the Kidma project, an organizational ICT project that failed after the investment of NIS 144 million, the IPS Commission and the Ministry of National Security have not examined the failure reasons nor drawn lessons in management preparations for future computerized projects and the realization of a new organizational ICT project in 2022 – the "Kabarnit" multi-year plan.

- **The Israel Prison Service's ICT Array and Technological Governance –** in 2014–2021, after the failure of the Kidma project, the IPS organization's management was limitedly involved in the ICT array. In 2018–2021, the IPS scope of the technology budget decreased (13%) while the overall budget of the IPS increased by 12%, and the average technological budget of government ministries increased by 25%. Moreover, core positions were partially staffed (the Head of the Technological Division and the Head of the ICT Department in the division). Furthermore, a substantial technological gap was found because of a lack of ICT infrastructures, which did not allow responding to the functional needs and challenges of the organization. As a result, a large part of the management routine of the prisons was done manually. The organization's control systems did not respond to its operational and administrative needs; The means of identifying the prisoners, the array of cameras, and the technological infrastructure on which the organization was based were outdated. This situation adversely affected the functioning of the IPS and its ability to meet its goals.

- **Approval of the "Kabarnit" Multi-Year Plan and its Budget –** the IPS began implementing the "Kabarnit" multi-year plan without the approval of its total budget at half a billion NIS and the approval of the Ministry of National Security and the Minister of National Security for its full implementation. Therefore, the IPS has begun implementing a comprehensive ICT program, with the approval of only about 20% of the total budgetary – NIS 532 million (of which about NIS 400 million is a technological

component), and without the approval of the level in charge of the plan as a whole. This poses a risk to the completion of the plan in the coming years. The IPS decided to implement the multi-year plan despite the lack of a budgetary source and without the Ministry of Finance and the Ministry of National Security committing to allocate the budget to the plan that would ensure its implementation.

- **Realization of the Technological Division Budgets of the "Kabarnit" Multi-Year Plan and Compliance with the Schedules for 2022 –** as of the end of December 2022, the IPS is behind in the realization of the projects in the "Kabarnit" multi-year plan that was planned for 2022. It was found that, out of a budget of NIS 104 million, about NIS 39 million, only 38% of the "Kabarnit" multi-year plan budget was realized. For about NIS 63 million, about 62% of the budget, purchase orders were issued, but the task was not completed. By a breakdown by projects, out of 31 technological projects in the "Kabarnit" plan, 24 projects are executed as planned, and 7 projects are behind schedule, among other things, as the budget from the Ministry of Finance was not received on time. The main projects whose implementation is delayed are the salary and personnel project, the server farm, the computerized prisoner file, visual conferencing with the courts, and the C&C system.

- **ICT Risk Survey –** despite the technological complexity of the IPS ICT array, the scope of the information systems, and their interfaces with government bodies, the IPS did not map the information assets, databases, infrastructures, and projects, nor did it conduct ongoing and comprehensive risk surveys. It was also found that the IPS did not perform comprehensive risk management of the "Kabarnit" plan for dealing with systemic risks in the budget, schedules, interfaces, infrastructure, technology, personnel, information security, assimilation, and the interdependence between the plan's components. A dedicated ICT risk manager was recruited only at the beginning of 2023.

**Investing in Technological Advancement –** after a long period of technological stagnation, starting in 2021, the IPS, and in particular its Technological Division, is investing considerable effort to catch up on the technology gaps by initiating and implementing projects to promote digitization at the operational and administrative core of the organization.

**Restructuring and Addition of Technological Personnel –** as part of the "Kabarnit" multi-year plan, a restructuring was carried out in the Technological Division. Furthermore, in 2022, personnel recruitment began and was largely completed, leading to a doubling of the personnel in the Division from 100 to 199 contractor employees.

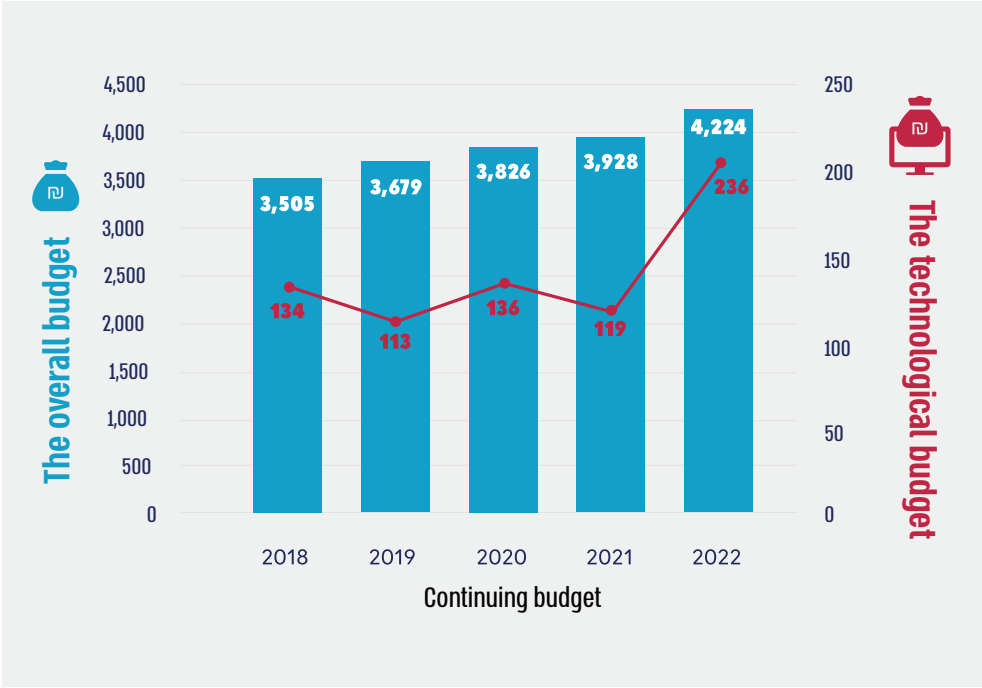
**Implementation and Integration of Technologies in the Operational Core Systems –** in 2022, the Technological Division, as part of the "Kabarnit" multi-year plan,

implemented new technological systems such as digital diaries, a digital prisoner file, and multidimensional monitoring systems as part of the transition to a "smart prison".

## Key Recommendations

- It is appropriate that the Israel Prison Service implement an organizational methodology of investigation and drawing lessons for future computerized projects. It is recommended that this process also apply to the "Kabarnit" plan as a whole, considering its cost and complexity. The Ministry of National Security, in charge of the IPS and guiding it, should be involved in these processes.
- It is recommended that the minister and the Ministry of National Security examine the "Kabarnit" plan for its approval, including the multi-year budget for its implementation. It is also recommended that the Ministry establish a regular and ongoing arrangement for monitoring the implementation of the program's core projects, including their goals, contents, timetables, and budgetary implementation. The performance of the "Kabarnit" plan, which is a multi-year and resource-intensive plan, requires the IPS to realize the plan after receiving approval from the Minister and the Ministry of National Security for the plan as a whole.
- The IPS should implement the National Digital Agency guidance and conduct a comprehensive and ongoing risk survey of all its activities, including the "Kabarnit" plan that was carried out at the audit time, and complete the project management staffing of the positions.
- It is recommended that the Ministry of Finance transfer development budgets ahead of time and not at the end of the budget year so that government bodies, including the IPS, can use these development budgets and issue orders in respect thereof at the same year, without being subject to budget cuts due to them being "committed surpluses." It is also appropriate that the Ministry of Finance, the Ministry of National Security, and the IPS examine the full range of implications of the "Kabarnit" plan's budget and the IPS technology budget, considering, among other things, the budget challenges at the audit time. All this is to ensure the implementation of the "Kabarnit" plan, given the importance of its completion.

## The IPS' Technological Budget Compared to the IPS' Overall Budget and its Changes, 2018–2022 (in NIS millions)




According to the IPS and Ministry of Finance data processed by the State Comptroller's Office.

# Part B – Information Security, Information, and Cyber Protection in the IPS

## The findings in this audit chapter are not made public to protect state security

The IPS, the national correctional organization that oversees 30 incarceration facilities, is a security body that holds thousands of criminal and security prisoners in custody. The information about these prisoners, including classified security information and sensitive personal information in the medical, biometric, and intelligence fields, is managed in the organization's information systems. Furthermore, the IPS computers store much information on modus operandi, operations, investigations, and information on the IPS defense and security systems. In addition to the information originating from the organization, the IPS receives classified, operational, and intelligence information from the Police and other agencies. The disclosure of this information to an unauthorized party may result, among other things, in harm to the state, risk human life, the disclosure of information, methods of operation, and covert investigations, and in the foiling of operations.

In recent years, a significant increase in cyber incidents has disrupted the everyday activities of organizations in Israel and worldwide. There is also a marked increase in the severity of these incidents.

# Key Findings

## The Regulation of Professional Guidance in Information and Cyber Protection

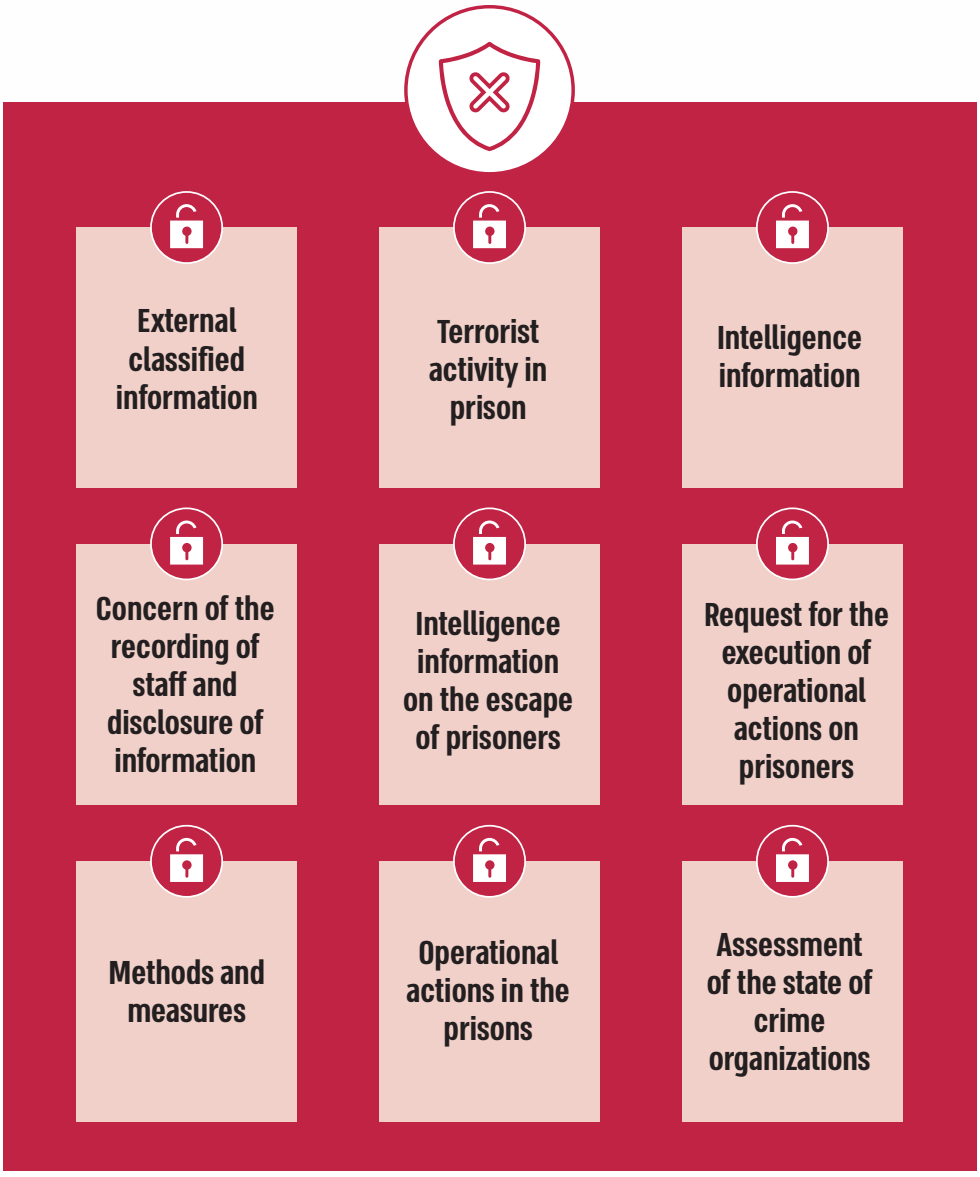
- **The Body Guiding the IPS in Information and Cyber Protection –** The IPS is a security body whose systems contain classified information at different levels. It was found that over the years, the IPS, the Ministry of National Security, and the National Cyber Directorate were not aware of the rules established in 2004 by the Prime Minister, which assigned the IPS with the responsibility of determining for itself the methods of securing classified information under the principles defined. Therefore, regarding the classified data, which embodies the highest risk, the IPS did not act under the binding rules or lay the necessary foundation for handling this sensitive field. In addition, the IPS did not receive support and guidance on classified data, even though regarding its

unclassified data, which embodies a lower risk, it received support and guidance from the sectoral unit in the Ministry of National Security. Moreover, despite the Israel Prison Service being a security body and the sensitive information in its possession, the Top Steering Committee for the Protection of Critical Computerized Systems (Committee B/84) did not discuss the IPS. It did not examine whether it should be defined as a "critical" body needing cyber Protection.

- **The Cyber Protection Policy –** the IPS was obliged to publish an organizational cyber security policy under the government's resolution in 2015. It was raised that at the audit completion in December 2022, the policy was approved for publication by the Deputy Commissioner as an organizational thematic doctrine but has not yet been approved by the sectoral unit in the Ministry of National Security. Furthermore, the approved sectoral policy document, which was published by the Ministry of National Security and which is intended, among other things, to direct and guide the bodies under its responsibility in cyber protection, is partial and does not include detailed instructions, adapted to accepted norms in the cyber Protection, for the bodies under its responsibility. The lack of these instructions affects the ability to ensure adequate preparedness of the IPS to cope with cyber-attacks.

- **The Management and Security of Classified Security Information –** one of the guiding principles for the security of classified information and documents is that there is a real need for compartmentalization and security measures to prevent the disclosure of security-sensitive information to an unauthorized party. The document's security sensitivity degree is determined by its classification level. Top Secret, Secret, Restricted, and Unclassified are the four classification levels.

## Examples of Information on the IPS Networks



The State Comptroller's Office examined a series of management and security aspects of classified security information. This examination raised significant gaps contrary to the binding practice in equivalent bodies. These gaps were found in each of the following areas:

1. Processing classified digital information and classified documents.
2. Regulating the handling of classified security information through security procedures, keeping and classifying documents.
3. Processing of classified information received from external sources.
4. Regulating the security clearance of employees in the IPS.
5. Use of means of communication.

## Protection of ICT Systems and Infrastructures

The State Comptroller's Office examined a series of protection of ICT systems and infrastructure aspects at the IPS. Penetration tests were also carried out with a vulnerability assessment survey of the IPS networks. Significant gaps were raised in this examination, contrary to the binding practice in equivalent bodies. These gaps were found in each of the following areas:

1. The cyber security of some systems.
2. Conducting risk surveys in information and cyber protection and conducting penetration tests.
3. Preparation for managing cyber incidents.
4. User management and permissions management.
5. The development processes of a classified computer network.

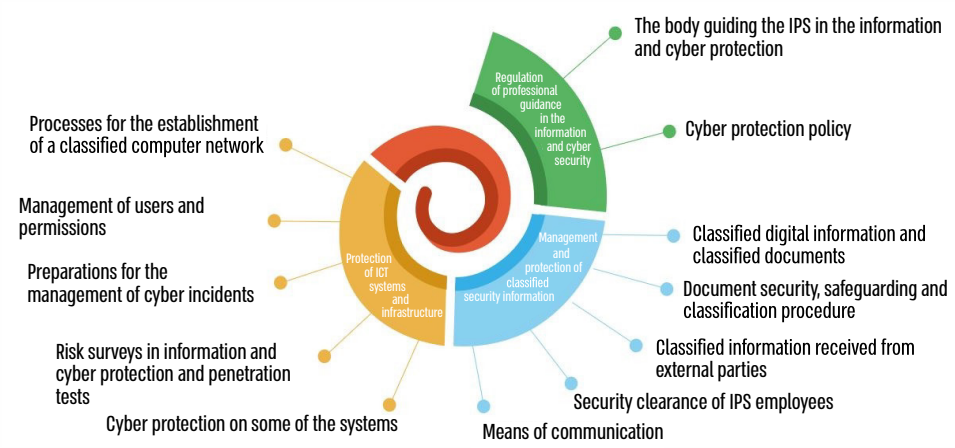
The extensive activity in the IPS Cyber Protection Department in recent years for implementing secure architecture and protection solutions is commended. This is despite the limited resources available to the IPS. This activity considerably improved information protection.

Furthermore, in 2021 and 2022, the IPS allocated over 8% of the organization's total annual information technology budget to the cyber security, meeting the minimum rate set by the government resolution.

# Key Recommendations

This chapter raised significant gaps in managing classified security information and its protection in the IPS computer systems. Moreover, the report raised a long-standing reality whereby the areas of responsibility and authority of the IPS and the regulators of classified information and cyber security, and in digital technologies and information systems, are not implemented, properly as required. It is recommended that the Prime Minister, in consultation with the Minister of National Security, examine the IPS information and cyber security as a whole, particularly the classified information security. Until the Prime Minister's decision, the IPS should comply with ISA rules.

## The key Gaps in the Information Security, Information and Cyber Protection



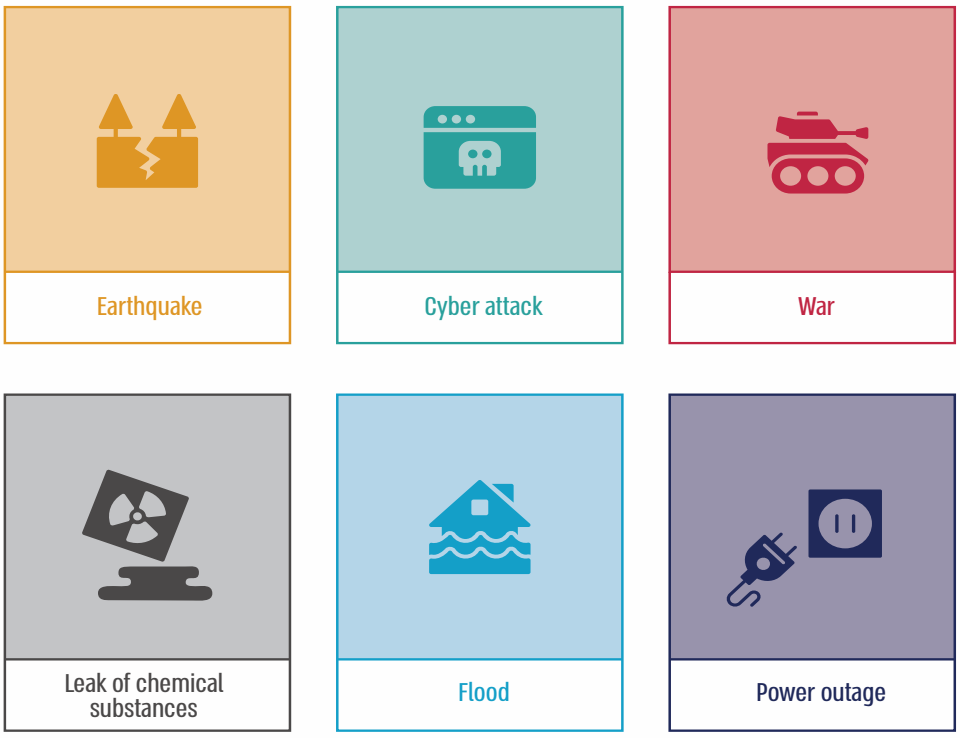

According to the audit findings, processed by the State Comptroller's Office.

# Part C – The Functional Continuity of the IPS Technological Systems and its Effects on the Prisons Functioning in the Event of a Disaster

## The findings in this audit chapter are not made public to protect state security

The functional continuity of the IPS in a variety of critical administrative and operational processes, including the security of the prisons at all levels, including the management of the intelligence system, the management of the day-to-day routine in the prison, including the counting of prisoners, distribution of medication to prisoners, personnel management, all depends on the technological systems. This continuity may be affected by a disaster or a severe crisis, whether it is a crisis that can sometimes be expected (such as a severe storm or extreme weather) or whether it is an unexpected crisis (such as a power outage, earthquake, terrorist event, war or accident) that disrupts the organization's routine. These events may also cause severe damage to the organization's technological system and create failures therein. Severe damage to the technological system can also result from physical damage (in good faith or with malice) or cyber-attacks on the organization's technological infrastructures and systems. Since the IPS is required to keep prisoners in safe custody even during an emergency or disaster, it should be prepared and ready for various emergencies and provide a response of functional continuity in any situation.

**The Main Disasters at the Basis of the IPS' Threat Reference**




# Key Findings

The State Comptroller's Office examined a long series of the functional continuity of the technological systems aspects in the IPS and their effects on the functioning of the prisons in the event of a disaster. The examination raised significant gaps contrary to the binding practice in equivalent bodies. These gaps were found in each of the following areas:

1. The technological response to the threat reference.
2. The Business Continuity and Functional Continuity Plan at IPS.
3. The Disaster Recovery Plan at IPS.
4. Protection of a sensitive IPS site and its operation.

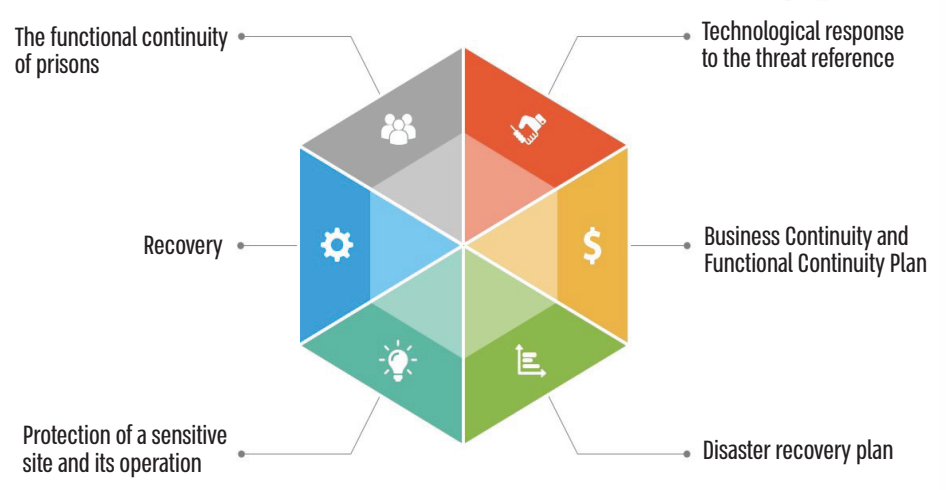
5. Data recovery and information systems recovery from backup.
6. The functional continuity of the prisons.

The IPS effort to promote and prioritize the establishment of the new server farm is commended.

# Key Recommendations

The functional continuity of the IPS is of strategic importance in terms of the lives of the prisoners in its custody and the guards entrusted with their custody and in the security and social aspects. The IPS and the Ministry of National Security should rectify the gaps raised in this chapter and implement detailed recommendations, all to ensure that this continuity is not affected by the occurrence of catastrophic events that may endanger the stability and functioning of the national correctional organization.

**The Key Gaps in the Functional Continuity of the IPS Technological Systems and its Effects on the Functioning of the Prisons in the Event of a Disaster**




According to the audit findings, processed by the State Comptroller's Office.

# Summary

The Israel Prison Service provides safe custody of prisoners and criminal and security detainees under adequate conditions while maintaining their dignity and rehabilitation toward integration into society following their release. Advanced technological systems support prison systems operating worldwide in realizing these organizations' mission. The role of the IPS, realizing its mission and security nature, requires it, similar to prisons around the world, to use advanced technological systems.

The IPS organization's management was limitedly involved in information technologies; moreover, a low technology budget, partial staffing of core positions, and a substantial technological gap affected the IPS's functioning and ability to meet its goals. At the end of 2021, the IPS was in a significant technological lag, in contrast to the benefits inherent in technological means as a tool to improve its ongoing administrative and operational functioning. In 2022, changes were executed to minimize the organization gaps to achieve a technological leap. The IPS, led by the Commissioner, adopted a comprehensive multi-year plan to improve the technological array. It even began its implementation in 2022 while receiving partial budgets from the Ministry of National Security and Finance. However, the plan, which was defined as a multi-year plan, did not receive the approval of the Minister of National Security on time and was only budgeted for its first year without a commitment being made by the Ministry of Finance and the Ministry of National Security to continue its budgeting in the coming years and to ensure its full realization.

The Minister and the Ministry of National Security are responsible for the functioning of the incarceration array in Israel, and they should ensure that the IPS fulfills its role through appropriate technological infrastructure and that the building up of that force is managed with a long-term vision and a budget outline that guarantees its implementation. In cooperation with the Ministry of National Security and the Ministry of Finance, the IPS should continue to reduce the existing technological gaps and place the IPS at an advanced technological level that matches its responsibility and mission as a security organization. The IPS should execute an orderly process of drawing lessons from previous failures in this area, manage ICT risks in general and the "Kabarnit" multi-year plan in particular, and provide a supportive professional management environment for its implementation.

This report also highlights significant gaps in managing classified security information and its security in the IPS computer systems. Despite the IPS being a security body, the computing infrastructure does not comply with the standards required of security bodies. The report raises a long-standing reality whereby the responsibility and authority of the IPS and the regulators in the classified information and cyber security, and the digital technologies and information systems, are not implemented properly and as required. This report is a warning sign for all bodies involved in securing state secrets, information, and cyber security and requires quickly rectification of the gaps raised therein. It is recommended that the Prime Minister, in consultation with the Minister of National Security, examine the information and

cyber protection in the IPS as a whole, particularly the classified information security. Until the Prime Minister's decision, the IPS should comply with ISA rules.

The functional continuity of the IPS is of strategic importance in terms of the lives of the prisoners in its custody and the guards entrusted with their custody and from the security and social aspects. The IPS and the Ministry of National Security should ensure that this continuity is not affected by catastrophic events that may endanger the stability and functioning of the national correctional organization.

It is recommended that this report be studied and that lessons be drawn from it for other government bodies of a similar nature in information security, information, and cyber security, as well as functional continuity of the technological systems and disaster preparedness.

State Comptroller's Report – Cyber and Information Systems | May 2023

The Ministry of Justice – Enforcement and Collection Authority

# Privacy Protection and Information Security in the Center for Collection of Fines, Fees and Expenses Systems in the Enforcement and Collection Authority

# Privacy Protection and Information Security in the Center for Collection of Fines, Fees and Expenses Systems in the Enforcement and Collection Authority

## Background

The Center for the Collection of Fines, Fees, and Expenses in the Enforcement and Collection Authority (the Center for Collection of Fines or the Center) collects debts for the State Treasury and public bodies and compensation awarded to victims of crime in criminal proceedings. As of February 2023, the debt balance in the open cases at the Center for Collection of Fines was about NIS 6.8 billion. The Center was granted collection powers to collect debts, including demanding information about the debtor from a public body. To effectively collect debts, the Center work is managed through a computerized system containing a large-scale database of about 3 million debtors, including, among other things, names, identity numbers, residential addresses, telephone numbers, details of debtors' assets, information from the National Insurance Institute, from the Licensing Division of the Ministry of Transport and other authorities.

As far as the privacy protection and information security is concerned, the Center for Collection of Fines is required to comply with the provisions of the law, including the Privacy Protection Law, 1981, and the regulations promulgated thereunder, government resolutions and the procedures and guidelines of the bodies that regulate the issue, including the Unit for Cyber Protection in the Government, which is a professional guiding body in cyber protection.

## Key Figures

**3 million**

the number of debtors included in the Center for Collection of Fines' databases

**about NIS 6.8 billion**

the total debt balance in the open cases in the Center for Collection of Fines

**only 7%**

the rate of unusual events[1] (99 out of 1,391) in September 2022 examined by the Center's control factors

**52%**

the access permission rate (23 out of 44) to the Center's operational system given without requesting the approval of the access permission Administrator at the Enforcement and Collection Authority

**14 access permission**

of employees of the information call center to the Center's database were not revoked despite the termination of their employment, within one to 13 months before the audit date

**21%**

the information call center employees rate (20 out of 94) who used the system without a smart card associated with them

# Audit Actions

From September 2021 to October 2022, the State Comptroller's Office audited aspects of Privacy Protection and information security in the Center for Collection of Fines systems. The audit examined the access documentation, the use of the information systems and the changes therein, the set of access permissions to the information systems in the Center, and contending with penetration risk into the information systems. Completion examinations were carried out in January and February 2023.

The audit was conducted at the Center for the Collection of Fines, Fees, and Expenses at the Enforcement and Collection Authority and the Authority's headquarters. Completion examinations were conducted at the Privacy Protection Authority at the Ministry of Justice and the Unit for Cyber Protection in the Government (Yahav) at the National Digital Agency.

1 Business events defined as unusual events in the operational system of the Center for Collection of Fines and warrant individual examination whether they were justified, such as closing a debt above a certain sum without payment.

At the same time, the State Comptroller's Office examined further activities of the Center, such as: managing the debt collection process from the stage of entering the case, sending payment demands, and performing various collection procedures; The debt rescheduling mechanisms, reductions and addition of arrears and the cancellation of debts; The management of the debt collection process of compensation for crime victims and the Communication with the crime victims. These audit findings were published in the State Comptroller's report from May 2023[2].

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

# Key Findings

- **Documentation of the Access to Information Center's Systems and Control Over it –** the Center for Collection of Fines does not document the users access to its system, to the extensive and sensitive information it holds and does not control it. Thus, in the event of user anomalies, it is impossible to detect them and stop them.
- **Examination of Unusual Events in the System –** although in 2016, the Center defined a list of 13 unusual events that require individual examination if justified, in September 2022, 1,391 unusual events were recorded, of which only 99 (7%) were examined. In addition, since 2016, the Center did not update the list of unusual events in the system.
- **Management of Access Permissions to the Center's System –** out of 44 user access permissions given in the dedicated computerized system (system B) in 2021, 23 (52%) of them were given without requesting the approval of the access Permission Administrator, as required by the Center's procedure.
- **Control of the Active access Permissions in the Center's Operational System and their Scope –** starting in July 2020, the beginning of the Center's using System B, and until the audit completion in October 2022, no control was performed on the access permissions to the system, nor the requirement to revoke permissions (due to inconsistency with the nature of the position or due to a change of position).
- **The Access Permissions Scope to the Center's operational system –** all the Center's employees, and the information call center employees who are outsourced, have

2 State Comptroller, **State Comptroller's Annual Audit Report, May 2023**, "The Center for the Collection of Fines at the Enforcement and Collection Authority", p. 1723.

access to the complete information in the operational system, containing about millions of debtors, without examining whether the scope of access to the information is necessary according to their position description.

- **The Access Permissions Management of the Information Call Center Employees –** the access permissions of 14 former call center employees to the Center's operational system were not revoked despite the termination of their employment within one to 13 months before the audit date. Furthermore, the Center did not block the smart cards of employees who no longer work there, and in practice, in different cases, the call center employees uses the cards and passwords of these employees.

- **Management of Permissions Access to System C –** access permissions to System C, generating cross-sectional reports on the Center's activities and detailed information on individual cases, were given to employees whose position nature does not require access to the information in the system. About 40% of the holders of permissions to System C (20 out of 52) did not use System C, at least since 2021.

- **The Enforcement and Collection Authority's Contending with the Penetration Risk into the Center Operational System –** in a penetration test carried out by Yahav, deficiencies were found at the infrastructure level that could pose a significant risk if a penetration into the organization's network occurred. The audit raised that despite the above findings, the Enforcement and Collection Authority did not implement a specific dedicated technological security solution in its systems, including in the Center's operational system.

# Key Recommendations

- The Center for Collection of Fines should establish a system to document the users access to the information in the operational system and periodiclly control the access under the provisions of the Information Security Regulations and the ISO 27001 standard (which is an international standard that addresses the establishment of a system for managing organizational information security and the ongoing process of system management and improvement).

- The Center should carry out quality and regular control over unusual events. It is also recommended to consider improving the list of unusual events in the system.

- The access permission Coordinator should avoid applying access permissions without the access permission Administrator's approval.

- The Enforcement and Collection Authority should examine the scope of the access permissions to the Center's operational system of employees in the various positions and

periodically control them under Yahav's directives and the Enforcement and Collection Authority procedures.

- It is appropriate that the Center consider limiting the access possibilities of the information call center employees to the information in its operational system based on the inquiries received at the center. In addition, it should periodically control the access permissions of the call center employees and refrain from using the system access permissions of employees who are not employed at the call center or from transferring smart cards from one employee to another.

- It is recommended that the Enforcement and Collection Authority individually examine the access permissions granted to System C according to the need and relevance to the permission holder position, thus reducing the access permission holders scope to the minimum necessary.

- The Enforcement and Collection Authority should promote the tendering process and implement a specific dedicated technological security solution, ensuring maximum protection of the information assets of the Enforcement and Collection Authority under Yahav's directives.

## The Procedure for Granting Access Permissions in Practice for the Center's Operational System


According to the Center for Collection of Fines' data, processed by the State Comptroller's Office.

# Summary

This report presents deficiencies in the privacy protection and information security in the information systems of the Center for Collection of Fines of the Enforcement and Collection Authority, including the lack of documentation of users' access to the information in the Center's operational system and consequently, the lack of control over that access; Failure to perform adequate monitoring of unusual events in the system; Poor management of the process of granting access permissions to the Center's operational system and of their supervision and control; Unlimited scope of access of the system users to its information; Inadequate management of the information call center employees' access permissions to the system; As well as the risk of external attackers penetrating the Center for Collection of Fines' systems.

These deficiencies are not in line with the provisions of the law, including the Provacy Protection Law and the regulations promulgated thereunder, the relevant government resolutions, and the guidelines of the bodies regulating the matter. This is reinforced given that the Center's operational system is classified as a database requiring a high level of security by the provisions of the Information Security Regulations,.

The Enforcement and Collection Authority and the Center should quickly follow the instructions of the relevant bodies to prevent the leaking of information from the organization and maintain its integrity. In addition, they should establish a system for documentation and control regarding using the Center's information systems. Furthermore, they should periodically control the access permissions of the Center's employees and even examine the access scope of the permissions to the Center's operational system by employees in various positions. Moreover, they should control the access permissions of the call center employees, and it is appropriate that the Center consider limiting the access of the call center employees to its operational system. Additionally, the Enforcement and Collection Authority should promote the tendering process and implement a specific dedicated technological security solution in its systems, ensuring maximum protection of its information assets.

The Center's extensive database includes sensitive information of about 3 million debtors. The debt sums handled by the Center as of the audit completion was about NIS 6.8 billion. Hence, the need to maintain the information systems to prevent damage to the integrity of the information and functional continuity of the Center for Collection of Fines in providing services, and to prevent the leaking of information from the database or to prevent their disclosure to unauthorized parties.

State Comptroller's Report – Cyber and Information Systems | May 2023

The National Insurance Institute

# Regulation of Cyber Security at the National Insurance Institute

# Regulation of Cyber Security at the National Insurance Institute

## Background

In 2021, more than 22 billion records were leaked worldwide due to cyber-attacks[1]. People's names and social security numbers (including SSN[2]) are the two data types that were leaked more than any other data. As of November 2022, about 2.9 million cyber-attacks are carried out daily against the National Insurance Institute (NII), of which about 66,000 attacks have the potential for damage.

The NII provides various services to residents of the State of Israel from birth to death. Therefore, the NII's databases are susceptible, both due to their enormous volume and because the databases interface with parties outside of the NII. Hereby are the normative regulations of cyber and information security: The Protection of Privacy Law, 1981, which defines the duties of the Database Owner, the Database Possessor or Database Manager as defined in the law, to secure the information therein; The Protection of Privacy (Data Security) Regulations 2017; And the Regulation of Security in Public Bodies Law, 1998 (the Regulation of Security Law), which establishes powers and responsibilities for physical security, information security and the security of vital computer systems of various public bodies, both of government entities and privately owned entities.

1 2021 Year End Report – Data Breach Quick View, Risk Based Security & Flashpoint (p. 3)

2 Social Security Number (it should be noted that in several countries such as the USA, the SSN number is equal to an ID number in Israel).

## Key Figures

**22 billion records**
were leaked worldwide in 2021 due to cyber attacks

**about 2.9 million**
the daily average of cyber-attacks on the NII

**hundreds of terabytes (TB)**
the size of the NII's database, which includes the personal data of about 9.5 million insured in Israel

**20 employees**
at the NII (of which 6 are students) supervise the information security in its computerized systems. Compare to the IDF, which is also self-supervised, has a Computer and IT Directorate (network environment) under the command of an officer with the rank of colonel

# Audit Actions

From October to December 2022, the State Comptroller's Office examined cyber protection regulations in the NII. The examination included mapping the bodies that currently regulate the NII, the possible damage from the lack of a fixed regulatory body, and the need to change the regulatory bodies. The audit was conducted in the NII, the National Cyber Directorate, the Israel Security Agency, and the Privacy Protection Authority in the Ministry of Justice.

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

# Key Findings

**The Regulation of the Privacy Protection Authority vis-à-vis the National Insurance Institute –** the audit raised that since the establishment of the Privacy Protection Authority in 2006 and until the audit completion (more than 16 years), the

Privacy Protection Authority has carried out six administrative procedures regarding information security in the NII. As for transversal supervision, only in August 2022 did the Privacy Protection Authority begin to conduct it in the NII.

- **The Regulation of the Israel Security Agency and the Interface of the National Cyber Directorate vis-à-vis the National Insurance Institute –** the Second Schedule to the Regulation of Security Law lists the bodies required to receive guidance regarding issues classified as top secret. These bodies carry out self-supervision and have dedicated units to protect cyberspace. The Fifth Schedule to the Regulation of Security Law lists entities with critical cyber infrastructure (CCI). These entities are guided by the National Cyber Directorate (NCD). It was raised that the NII is indeed listed in the Second Schedule but is not defined in the Fifth Schedule to the Regulation of Security Law, even though it is a body that maintains a database of information on the residents of the State of Israel. Therefore, the NII receives directives from the Israel Security Agency regarding classified issues only but is not required to receive regular instructions from the NCD.

- **The "Voluntary Instruction" Process of the National Cyber Directorate –** as of 2016, the NCD began instructing the NII under "voluntary instruction." I.e., the NCD instructs the NII similarly to the CCI bodies, but the NII has no obligation to implement these instructions. From the audit team's conversations with the NII, it became clear that the NCD's level of involvement over the years has decreased: from 2016 to 2020, the "voluntary instruction" was tight and included ongoing consultation daily. From the end of 2020, three supervisors have come and gone, and instruction has been sparse and sporadic. At the audit completion, there is no supervisor on behalf of the NCD, and contact is carried out through the NCD call center (CERT), which handles all cyber incidents in Israel. Therefore, the NII does not have a regular and systematic response for handling all information security incidents.

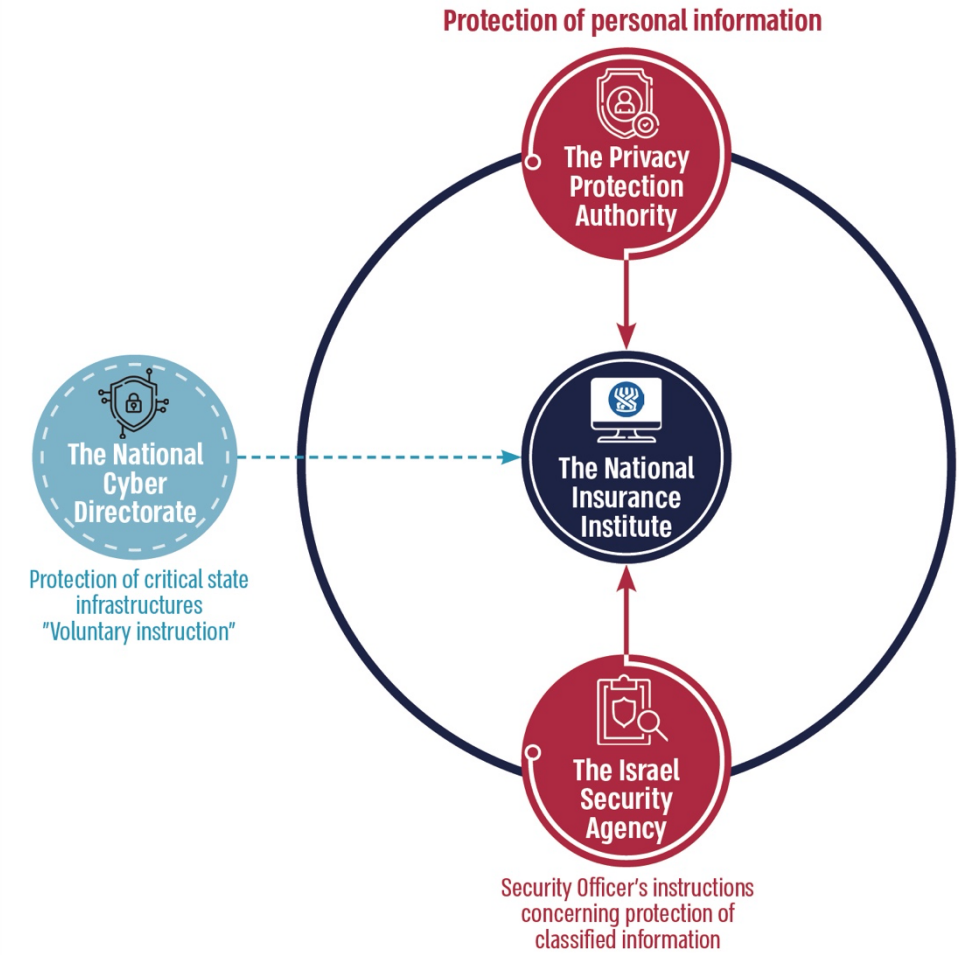
- **The Attempt to Define the NII as a Critical Cyber Infrastructure (CCI) –** Government Resolution B/84 from 2002 established a top steering committee[3] to examine which bodies are critical and, therefore, need cyber protection. It was found that as of the audit completion – about two years after a hearing in the Steering Committee for the Protection of Critical Computerized Systems resulted in a decision to examine the NII as a CCI body, the NCD did not begin the examination procedure. An inquiry by the audit team at the NCD raised that the NCD intends to start examining the NII as a CCI body in the first quarter of 2023. I.e., at the audit completion, the NII, which manages a database, does not receive ongoing and binding professional instruction, which raises a concern for risk.

3 The Chairman of the Steering Committee is the head of the NCD and its members include representatives from the Ministry of Defense, the Ministry of Justice – the Head of the Privacy Protection Authority, the National Security Council, the IDF and the Israel Security Agency.

# Key Recommendations

- It is recommended that the Steering Committee for the Protection of Critical Computerized Systems promote the examination of the NII as a CCI body, given the extent of the information stored therein and the risks of its leakage.
- It is recommended that until the end of the Steering Committee examination, for the Protection of Critical Computerized Systems, a professional interface will be established between the NCD and the NII to provide a direct response, forwarding reports, monitoring the correction of deficiencies, etc.
- It is recommended that the Steering Committee for the Protection of Critical Computerized Systems examine whether there are other entities with databases of a similar scope to the NII whose definition as CCI bodies should be considered, thus improving the protection of the State of Israel's critical infrastructures.

## Regulatory Bodies in the NII Information Security



# Summary

Like other countries, Israel is exposed to cyber-attacks for ransom and information theft. Apart from that, given the complex security geopolitical climate, Israel is an extensive target for a potential cyber attacker wishing to harm its resilience and national security. A body such as the NII requires a satisfactory regulatory response formulated, including guidance from the National Cyber Directorate and the Privacy Protection Authority and coordination between the two to ensure optimal protection. Given the volume of information kept at the NII and the risks of its leakage, it is recommended that the Steering Committee promote the examination of the NII as a CCI body. It is recommended that until the end of the examination, a professional interface between the NCD and the NII will be arranged to provide a direct response, forward reports, monitor the correction of deficiencies, etc. It is also recommended that the Steering Committee examine whether there are other entities with databases of a similar scope to the NII whose definition as CCI bodies should be discussed, thus improving the protection of the State of Israel's critical infrastructures.

State Comptroller's Report – Cyber and Information Systems | May 2023

Ministry of Health

# Cyber Audit at Medical Center A – Penetration Test on the Infrastructure and the Communication Network

# Cyber Audit at Medical Center A – Penetration Test on the Infrastructure and the Communication Network

## Background

Over the past decade, cyber-attacks on organizations and individuals worldwide have increased. In 2020, about 9.5 million attempted cyber-attacks were detected worldwide, the purpose of which was to disable computer systems and prevent the ability to use them[1]; 18 attempted attacks per minute were detected, on average; In the first half of 2020, at least 36 billion personal data items were stolen or leaked to the internet following cyber-attacks. Accordingly, cyber threats to the health system, including medical centers, have increased in recent years. Furthermore, the health sector was one of Israel's ten most attacked sectors in 2021[2].

Medical institutions use tens of thousands of medical devices for various medical operations. Among these devices are imaging devices such as magnetic resonance imaging devices (MRI), computed tomography (CT), X-ray, and ultrasound devices. The medical devices must be thoroughly and regularly available given the variety of medical operations performed, and especially given their necessity for life-saving procedures.

Cyber security (information security) in medical devices, including imaging devices, prevents an unauthorized party from making changes to the information stored in the medical devices; Unauthorized use or misuse of the medical information stored in the medical device, processed in it, or transferred from it to an external destination; As well as harm the operation of the medical device. One of the ways for an organization to prepare for cyber threats is to perform "resilience tests." These tests are designed to examine the organization's level of protection, locate security breaches and possible risks, and handle them accordingly. One of the resilient tests is a "penetration test" (PT) – a process in which a controlled and planned attack is carried out on the organization's computerized systems to find vulnerabilities.

In May 2022, the State Comptroller's Office performed a penetration test at a specific medical center (Medical Center A or the Medical Center). The recommendations for rectifying the deficiencies in this report are addressed to the Medical Center's management and the Ministry of Health, the regulator of the medical institutions, including in their information security, so that it examines the results of the penetration test, and implement the recommendations made as a result of it in all medical institutions.

1 DDOS – Denial of Service Attack Distributed attacks. The attacks and leaking of data were in various extensive fields.

2 The National Cyber Directorate, Year 2021 Summary.

## Key Figures

**9.5 million**
cyber-attacks attempts worldwide to disable computer systems were detected in 2020

**18 times a minute**
cyber-attack attempts were detected, on average, in 2020 worldwide

**36 billion**
personal data items were stolen or leaked online following cyber-attacks in the first half of 2020 worldwide

**1 of 10**
the health sector was one of the ten most attacked sectors in Israel in 2021

**over 100**
the State Comptroller's Office scanned in the infrastructural penetration test over 100 servers and endpoints of the medical equipment of Medical Center A

**10**
out of 13 findings in the State Comptroller's Office penetration test were of a "high" severity level. Three were of "moderate" severity

**NIS 10 million**
the annual estimated cost to rectify the deficiencies raised in the penetration test

**about NIS 36 million**
the Hillel Yaffe Medical Center restoration cost after the cyber-attack perpetrated in October 2021

# Audit Actions

In May 2022, the State Comptroller's Office published an audit report on "Cyber Security of Medical Devices and the Security of the Information Stored Therein"[3]. Following the above audit report, in May 2022, the State Comptroller's Office performed a penetration test on the infrastructure and the communication network that manages the medical equipment at Medical Center A. The penetration test was conducted with the assistance and accompaniment of an external consulting company. It was carried out in the production environment[4] of the network that manages the medical devices. The penetration test was performed in the format of a resilience test that included a risk survey and a scan of vulnerabilities and weaknesses in the system.

3 State Comptroller, **State Comptroller's Report, May 2022**, "Cyber Protection of Medical Devices and the Security of the Information Stored Therein", pp. 1133–1238.

4 The production environment – the work environment that serves the end users and includes software systems and other technological products.

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

# Key Findings

In the penetration test, 13 significant findings were found in five areas: segmentation and flow control, network access control, protection of workstations and servers, out-of-date software, and insecure access. Ten of the findings were of high severity, and three were of moderate severity.

**The Cooperation of Medical Center A's Management and the Deficiencies Rectifying –** the cooperation of the Medical Center's management in performing the test and rectifying the deficiencies is commended.

# Key Recommendations

It is recommended that the Medical Center's management examine all the medical devices and their supporting systems where deficiencies were found and regularly and habitually manage the risk involved in vulnerable equipment systems to minimize the risks. It is recommended that the management consider the restoration costs due to damage that may occur if these systems are not replaced and examine which systems to upgrade according to their priority. Regarding systems that cannot be upgraded or that will be prioritized as low priority, it is appropriate that the management consider implementing additional compensatory controls. All this is to mitigate the possible harm to the patient's lives and privacy.

It is also recommended that the management formulate an organization-wide work plan to eradicate the risks or minimize them when it is impossible to rectify the deficiencies that have arisen. It is also recommended to carry out penetration tests following a regular plan.

It is recommended that the Ministry of Health, which acts as the regulator in the health sector including information security, complete the penetration tests that it has begun in all medical institutions in Israel and establish a format for periodically performing penetration tests in all institutions. It is further recommended that the Ministry of Health

examine the penetration test findings carried out at Medical Center A and implement the recommendations based on the test findings in all medical institutions. It is also recommended that the Ministry of Health ensure that all medical institutions perform periodic penetration tests, examine the findings of the tests, follow up on rectifying the deficiencies found, and, accordingly, publish recommendations to all medical institutions. In addition, it is recommended that the Ministry of Health continue, as a rule, to help all medical institutions at the national level to cope with the challenges of information security regarding medical equipment.

## The Areas in which Deficiencies were Found in the Penetration Test (some were rectified by the audit completion)

Un secure access

Out-of-date software

Protection of workstations and servers

Network access control

Segmentation and flow control

# Summary

One of the ways to prepare for cyber threats is to perform penetration tests on the organization, to identify vulnerabilities in its defense and to minimize them, and when it is not possible to address the vulnerabilities that were found – to bring the potential risks to the attention of the organization's management and manage them on an ongoing basis. Following the penetration test, the management of Medical Center A rectified several deficiencies and, in particular, updated the security level of specific systems. According to the Medical Center's management, the total cost of rectifying the deficiencies may be over NIS 10 million annually on an ongoing basis. It is recommended that the management formulate an organization-wide work plan to eradicate the risks or minimize them when it is impossible to rectify the deficiencies found. It is also recommended to perform penetration tests following a regular plan.

The Ministry of Health is the regulator of medical institutions, including information security. It is recommended that the Ministry of Health, as the health regulator, complete the penetration tests it has begun to perform in all medical institutions in Israel and establish a format to perform penetration tests in all institutions periodically. It is further recommended that the Ministry of Health examine the penetration test findings carried out at Medical Center A and implement the recommendations based on the test findings in all medical institutions. It is further recommended that the Ministry of Health ensure that all medical institutions perform periodic penetration tests, examine the findings of the tests, follow up on rectifying the deficiencies found, and, accordingly, publish recommendations to all medical institutions. In addition, it is recommended that the Ministry of Health continue to help all medical institutions at the national level to cope with the challenges of information security regarding medical equipment.