OFFICE OF THE STATE
COMPTROLLER AND
OMBUDSMAN OF ISRAEL

STATE OF ISRAEL

State Comptroller Report

Cyber and Information Systems

Abstracts

May 2023

State Comptroller Report

Cyber and Information Systems

Abstracts

State of Israel

State Comptroller Report

Cyber and Information Systems

Abstracts

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