

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



December 2022 | Jerusalem

Catalogue Number 2022-S-003

ISSN 1948-0973

www.mevaker.gov.il

Graphic Design: ER Design Team



Table of contents

Abstracts

Foreword	7
Cyber Protection and Business Continuity in the Automated Processing Service Unit at the Tax Authority	11
Cyber protection in the Transport Sector	19
Management of Biometric Information in the IDF and its Cyber Protection	33
Establishing a New Foreign Trade System at the Tax Authority – the "Global Gateway" Project	47
Regulation and Supervision of Local Water Suppliers in Cyber Protection	59
Special Audit Report – Cyber Protection of Information Systems in the Ministry of Education and of Matriculation Exams and Grades	65



Foreword

The report submitted today to the Knesset is the first of its kind, and it presents the audit results in cyber protection, information technology and privacy protection.

Cyberspace includes computers, automated systems and networks, software, computerized information, digital content, traffic and control data. Cyberspace is characterized by rapid technological development, which permeates all areas of life and shapes mankind's social, economic and political activity. Cyberspace and technological progress hold many advantages for the economy and society, but they hold inherent threats that may affect the functional continuity of the organization, the integrity of processes and the confidentiality of organizational information.

Given the ever-increasing cyber threats, the State of Israel is facing in recent years, at the beginning of my tenure as State Comptroller and Ombudsman I specified the cyber field as one of the core issues the state audit will address. This is to examine the audited bodies' preparedness and readiness to contend with significant cyberspace risks, strategic threats and future cyber challenges that lie before them.

To develop and strengthen the professional abilities of the State Comptroller's Office in cyber and information systems, several key measures were taken, including the establishment of a cyber audit division dedicated to conducting audits in this field. In addition to the division dedicated recruiting employees with a unique professional background in the cyber field; Promoting the process of international certification of the Office's employees as certified information systems auditors (CISA); and the engagement of external consultants in information and cyber protection to accompany the audit teams in these areas.

Furthermore, as part of the cyber protection audit, the State Comptroller's Office carried out a precedent-setting step in Israel and among state audit institutions worldwide – penetration tests into the computerized systems of several audited bodies simulating a cyber-attack. The penetration test was done to find vulnerabilities in the computer system that may endanger its stability during an attempted attack, and as a result disrupt the regular functioning of the tested system. The tests were conducted in coordination with the audited bodies, and they already rectified some of the deficiencies that emerged during the audit.

In 2021–2022, the State Comptroller's Office carried out dedicated cyber and information security audits in infrastructure, education, transportation, health and financial fields and in local authorities. Among other things, the office examined the information systems and cyber protection as part of the election processes for the 21st, 22nd and 23rd Knesset; Biometric databases; Cyber protection for medical devices; And information systems management in local authorities. As part of the audits, the following topics were examined: the integrity and reliability of the information systems in the audited bodies; The effectiveness of the



computerized protections and controls embedded therein; The protection of personal and private information in government systems; Investment in IT; pre-preparedness for cyber incidents and disaster recovery; Preparedness for cyber-attacks and damage to critical state infrastructures and more. The chapters on these topics were made available to the public in our annual reports.

This report is unique as it deals entirely with the results of the state audit in information systems and cyber protection. Following are the chapters of the report:

- a. Cyber protection and business continuity in the Automated Processing Service Unit at the Tax Authority
- b. Cyber protection in the transport sector
- c. Management of Biometric information in the IDF and its cyber protection
- d. Establishing a new foreign trade system at the Tax Authority – the "Global Gateway" Project
- e. Regulation and supervision of local water suppliers in cyber protection
- f. Special audit report - Cyber protection of information systems in the Ministry of Education data bases and of matriculation exams and grades

The audit on the topics above raised the following deficiencies: user and permissions management; Documentation and monitoring of network access and control; Protection of stations and servers; Segmentation and flow control; Software updates; Adherence to secure access to systems, protection of personal information of millions of citizens and more.

In recent years, we have witnessed various types of cyber-attacks, ransomware and malware incidents, fraud, embezzlement and business information theft. The cyberspace has even become an arena for warfare between terrorist and criminal organizations and countries and even between countries themselves. In the coming years, a considerable increase in the penetration of cyberspace into the daily routine is expected, given the development of IOT (Internet of Things) products, autonomous cars, and more, and accordingly a considerable increase in the frequency of cyber threats and their degree of severity is expected.

The audited bodies are obligated to act in a quick and efficient manner to rectify the deficiencies raised in this report, to increase the organization's level of protection and to prepare for optimal handling of cyber-attacks; To adapt their activities to a world saturated with advanced technologies and to the challenges they will face in the coming years. 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 with dedication in carrying out audits in a



We at the State Comptroller's Office are obligated to continually examine the compliance of the audited bodies with current and future risks and engage in the cyber protection, information technologies and privacy protection, for the benefit of the citizens of Israel and the entire world.

Matanyahu Englman
State Comptroller and
Ombudsman of Israel

Jerusalem, December 2022



Report of the State Comptroller of Israel | Cyber and
Information Systems | 2022

The Israel Tax Authority

Cyber Protection and Business Continuity in the Automated Processing Service Unit at the Tax Authority



Cyber Protection and Business Continuity in the Automated Processing Service Unit at the Tax Authority

Background

The Automated Processing Service (Shaam) is a unit serving the Israel Tax Authority's IT (Information technology) system and providing it through computer services for collection and enforcement, creating proper deterrence and exhaustion of taxpayers' rights. Shaam serves about 1.3 million "customers": companies, other types of corporations, self-employed, controlling stakeholders, employees, and recipients of work grants, employees performing tax adjustments and tax refunds, 6,000 employees of the Tax Authority, 13,000 representative offices, and 7,000 lawyers. Shaam manages hundreds of projects every year, from projects for immediate execution to long-term projects. Shaam keeps the information about citizens, taxpayers, dealers, and other entities in its systems.

The law of Security in Public Bodies, 1998 determines the areas of authority and responsibility for physical security, information security, and the security of essential computer systems of various public bodies, including government and privately owned bodies. The law defines critical computer systems as "computer systems determined as essential by the body authorized to that by the government".

In 2010, a senior steering committee decided that Shaam would be included in the Second and Fifth Schedules for the Regulation of the Law of Security. Accordingly, the National Cyber Directorate was authorized to issue Shaam professional guidelines concerning securing essential computing systems.



Key figures

1.3 million

Shaam service recipients: companies, corporations, self-employed, employees, and more

part

of the Shaam employees who require security clearance do not have the required clearance

11

the number of findings of the penetration test conducted by an external consultant on behalf of the State Comptroller's Office

2014

the year in which the preparation of a business continuity plan began in Shaam and has not yet ended

Audit actions



From November 2021 to February 2022, the State Comptroller's Office examined Shaam's information security and cyber protection. The audit was conducted at Shaam, and completion examinations were carried out in the National Cyber Directorate.

The audit included the examination of some aspects of cyber protection, the penetration test of the system supporting a business process at the Tax Authority (System A), and Shaam's preparedness for business continuity and disaster recovery.

This report was submitted to the Prime Minister on July 31, 2022, and was classified as confidential until its discussion at the State Audit Committee's Subcommittee.

Under the authority vested upon the State Comptroller in Section 17(c) of the State Comptroller's Law, 1958 [Consolidated Version], considering the government's reasoning, consulting with the bodies entrusted with the security of defense information, in coordination with the Knesset chairman, and as the said subcommittee did not convene, it was decided to publish this report while classifying as confidential parts thereof. These parts were not brought before the Knesset and will not be published.

The audit report's findings and recommendations are correct as of the aforementioned date of its publication.



Key findings



- The steering committee's duties over critical computing infrastructures** – it was raised that the committee's responsibilities were defined in the letter of appointment in general terms and were not detailed as required by the regulatory guidelines. Moreover, the committee's discussions do not address the actions it should take according to its duties, as the guidelines require.
- Mapping processes and information assets** – according to the regulatory guidelines, Shaam should map the information assets and access routes to comply with a security plan. Gaps were found in mapping the processes and information assets carried out at Shaam, which does not fully comply with the regulatory guidelines' requirements.
- Discrepancies in Shaam procedures** – the audit found discrepancies in the regulatory guidelines in some Shaam procedures, among other things, regarding the work interface with the National Cyber Directorate.
 - **Changes management** – no reference was found in the relevant procedure to the need to update the appropriate party and include it in analyzing the risks and expected effects of the changes, as required by the guidelines.
 - **Procedure for handling information security incidents** – there is a procedure at Shaam but it does not refer to the obligation to report to the relevant party and the need to include it in the incident's investigation. In addition, there is no reference pertinent to an area required in the guidelines.
- Centralization of information regarding the supply chain** – gaps were found regarding the information collected by the Shaam Information Security Wing on the supply chain. Furthermore, Shaam did not use the supply chain module in the dedicated system developed by the National Cyber Directorate.
- Weakness in a particular server** – there were gaps in the control of a specific server.
- Required clearance** – the audit raised gaps between the clearance approval level needed according to some Shaam employees' duties and their level of approval in practice.



Penetration test on behalf of the State Comptroller's Office on System A

-  This system supports a business process at the Tax Authority. During the test, findings emerged that endangered the information from a business point of view and the organization's reputation.

Preparedness for business continuity and disaster recovery

-  **Regulation of the wing's activities** – in November 2016, Shaam's director decided to form an organizational structure that will be planned, with the assistance of consultants, to establish a quality and business continuity wing. The Civil Service Commission stipulated the wing approval of its necessity by the ICT Authority. It was raised that the wing has been operating since the end of 2016, although the Commission has not approved the organizational structure change. The job definitions of the wing employees are the definitions of their previous positions, and they are employed according to the headcounts assigned to other wings. Consequently, the wing authority and its duties are not regulated.
-  **Disaster recovery plan** – the disaster recovery plan includes a plan for the recovery of the technological array, the process of activating emergency mode, the process of coming back from emergency mode to routine, the emergency drills, and the main indices for recovery:
 - Return Point Objective (RPO) – the volume of information lost during a disaster.
 - Return Time Objective (RTO) – the maximum time from the moment the decision is made until the emergency site is activated.
 - Gaps were found regarding the completion of a disaster recovery plan.
-  **Business continuity plan** – gaps were found in formulating a business continuity plan and in its completion.



Key recommendations

-  It is recommended that Shaam rectify the deficiencies found in mapping the processes and the information assets.
-  It is recommended that Shaam update its procedures and include all the necessary actions according to the regulatory guidelines.
-  It is recommended that Shaam use the dedicated system developed by the National Cyber Directorate to examine the supply chain.
-  It is recommended that Shaam ensure that the clearance level of all Shaam employees is adapted to their positions.
-  It is recommended that Shaam examine the findings of the penetration test conducted on behalf of the State Comptroller's Office and rectify the deficiencies raised in this report.



Summary

Shaam is the Tax Authority's IT body. Hence, it develops information systems, maintains existing systems, and holds information. It is of great importance that Shaam will have a high level of cyber protection, that functions fully in times of crisis, and rapidly recover from disaster.

By the audit findings, Shaam should improve the cyber protection of its systems.

It is recommended that Shaam rectify the deficiencies raised in this report as soon as possible and consider the implementation of the report's recommendations.



Report of the State Comptroller of Israel | Cyber and
Information Systems | 2022

Ministry of Transport and Road
Safety

Cyber Protection in the Transport Sector



Cyber Protection in the Transport Sector

Background

The Ministry of Transport and Road Safety is setting the policy in the Transport sector and the services of the Transport systems at sea, air, and land. The Transport sector includes entities of various types – governmental, public, and private, operating in various fields: maritime transport, land transport, air transport, public transport, transport infrastructures, and smart transport.

In recent years, there has been a sharp increase in the number and severity of cyber incidents disrupting the everyday activities of organizations in Israel and around the world. In transport, many risks may materialize because of cyberspace vulnerabilities: damage to Transport infrastructure and means of mass Transport that may result in loss of human life, interruption of production processes, heavy economic damage, personal information leaking, security to the organization reputation and in some cases even potential security consequences.

By Government Resolution 2443 from 2015, the government ministries, including the Ministry of Transport, should promote preparedness for cyber threats in their sector. In this framework, the Ministry of Transport established its Cyber Division to guide the entities in the sector, except for entities defined as Critical State Infrastructures (CSI) that the National Cyber Directorate directly steers.

Sectoral regulators can compel entities steered by them to comply with cyber requirements in several ways: laws and regulations, stipulating the granting of a license on compliance with cyber requirements, issuing guidelines, and including cyber requirements within the framework of engagements. The Ministry of Transport instructed the entities in the sector to comply with the cyber requirements included in the Cyber security Policy.



Below is a chart describing the areas of operation in the Transport sector:





Key figures

28,000

entities operating in the Transport sector, including private vehicles, infrastructure, public transport, aviation, and sea transport

4 out of 5

the privacy threat rating determined by the Privacy Security Authority regarding transport

6 out to 30 7 years

20% of the entities defined as critical state infrastructures holding essential computerized systems belong to the Transport sector

the delay in the Cyber Law enactment, still not completed, according to the requirements in Government Resolution 2444 of 2015

NIS 36 million

the Ministry of Transport's development budget for 2022

NIS 6.3 million

the Cyber Division budget approved out of the total requirements it submitted – NIS 30 million (21%) as of December 2021

21 out of 35

60% of the entities which are planned to be connected to the Sectoral Information Security Incident Monitoring Center (SOC), but by the audit completion, were not connected to it

0%

the entities rate that performed penetration tests to detect security vulnerabilities in Transport systems in 2019–2021 (0 out of 8 audited entities)

Audit actions

 From March 2021 to April 2022, the State Comptroller's Office audited cyber protection in the Transport sector. The audit was conducted at the Ministry of Transport – in the Cyber Division and the Legal Counsel Department; at the National Cyber Directorate in the Prime Minister's Office – in the Division for Sectoral Guidance and in the Unit for Guidance of Critical State Infrastructures Entities (CSI Division) and at the Privacy Security Authority in the Ministry of Justice. Completion examinations were done in several government companies and the sectoral cyber security units in the Ministry of Energy, Environmental Protection, Communications, and Ministry of Health.

As part of the audit, the State Comptroller's Office, in collaboration with Municipality A, carried out an innovative process – a penetration test of its transport systems to examine aspects of cyber protection.



The Office also distributed to ten municipalities and two government companies a questionnaire examining on a systemic level the cyber security in transport systems.

This report was submitted to the Prime Minister on July 31, 2022, and was classified as confidential until its discussion at the State Audit Committee's Subcommittee. Under the authority vested upon the State Comptroller in Section 17(c) of the State Comptroller's Law, 1958 [Consolidated Version], considering the government's reasoning, consulting with the entities entrusted with the security of defense information, coordinating with the Knesset chairman, and as the said subcommittee did not convene, it was decided to publish this report while classifying as confidential parts thereof. These sections will not be brought before the Knesset and will not be published.

The audit report's findings and recommendations are correct as of the aforementioned date of its publication.

Key findings

-  **Regulation at the level of primary legislation** – as of audit completion in April 2022, the legislation of the Cyber Law was still not completed seven years after the Government Resolution 2444 was taken. The cyber domain regulation was also not completed as part of the work of the inter-ministerial team established in August 2021. Given the above, each regulator including the Ministry of Transport should independently amend its laws and regulations to implement cyber requirements in its sector.
-  **The introduction of cyber requirements into regulations and laws in the transport sector** – during the last seven years, the Ministry of Transport has not completed the administrative work for the examination of the regulation changes and amendments required to exercise the responsibility for cyber security in its sector effectively. The Ministry of Transport preferred to wait for regulation of the Cyber Law, except for autonomous vehicles, even though the said legislation was delayed. Hence, the Ministry of Transport lacks the tools to enforce the cyber requirements it established on the entities in the sector (including public transport operators, seaports, and airlines).
-  **The introduction of cyber requirements for engagements with transport operators** – in September 2021, the Ministry of Transport introduced mandatory cyber addendums in new land infrastructure engagements; however, in some areas, the Ministry does not require the inclusion of cyber-related requirements in new engagements. It should be noted that in the Ministry's areas of operations, some agreements are signed for an extended period, while the agreements signed in the past



do not include cyber requirements. For example, seaports – a 25-year concession; operating public transport clusters – 10 years. It was also raised that the Ministry has no centralized map of the existing engagements, including their termination dates, and it does not know whether cyber requirements are included in these contracts. Given this situation, there is a risk that even contracts expected to end shortly will be extended without the addition of cyber requirements as part of their extension and renewal.

-  **Examining the state of cyber security in large transport entities by the Ministry of Transport** – in 2021, the Ministry of Transport examined the compliance level of some of the entities with the cyber requirements it published including the Cyber Security Policy for the sector. The examinations were conducted on companies in various fields, including public transport companies, road infrastructure companies, and seaports. The examinations found a series of cross-organizational deficiencies that require systemic measures. However, the Ministry did not follow up on rectifying the deficiencies noted in them.
-  **The Cyber Division's resources** – the human resources and the budget necessary for the Ministry of Transport to fulfill its cyber responsibilities are insufficient (for example, the Division employs three employees instead of five, and only NIS 6.3 million (21%) of the budget the Division requested to fulfill its role were approved), so it cannot respond to some of the threats facing it. Due to the lack of resources, it was found that some of the Cyber Division's tasks were not carried out, including the ability to intervene in cyber incidents; increasing resilience in the sector; expanding audits of the sector's entities; and supporting them in rectifying severe deficiencies.
-  **Compilation of a sectoral situation report** – the Ministry of Transport is responsible for promoting preparedness for cyber threats in the entire sector. Still, it has difficulty fulfilling its responsibilities for the following reasons: the Ministry cannot see the whole sectoral picture of all its sub-sectors (for example, the field of air transport and the CSI entities that are under the guidance of the National Cyber Directorate); it does not have a risk map and the disparities existing in each entity; and it does not receive from them essential information about the activities they performed, such as penetration tests, work plans to rectify the deficiencies, reporting on cyber incidents and investigating them. Furthermore, discrepancies were found in some cyber incidents reported to the various authorities.
-  **Information Security Incident Monitoring Center (Sectoral SOC)** – 21 out of 35 of the entities planned to be connected to the Sectoral SOC established by the Ministry of Transport were not connected to it by the audit completion, and no detailed work plan was formulated for the connection of all the entities and for their becoming operational. It was also raised that the Ministry of Transport's current engagement with the IAA on the SOC operation was signed for one year only and did not provide a complete response to large organizations.



-  **Information sharing** – it was raised that sharing cyber information between similar entities (such as seaports and transport systems) is partial. It was also found that there is no template for publishing tenders in cyber for use by entities in the sector.
-  **Guidance of systems in the field of transport** – an urban transport system is responsible for transport within its city jurisdiction. In a survey conducted by the State Comptroller's Office in ten municipalities and two companies, substantial gaps were found between the cyber security status of the systems and the Ministry of Transport's cyber requirements. It was also found that not all the transport systems (except those operated by the infrastructure companies and Municipality A) receive instructions from the Ministries of Interior or Transport, although there are those whose damage may cause considerable economic harm and even loss of life.
-  **Penetration tests and risk surveys on transport systems** – by the questionnaire results on cyber security sent to entities with urban and intercity transport systems in 2019–2021, none of the entities examined performed penetration tests, and 75% of the entities examined did not perform risk surveys.
-  **Business recovery, testing environment, and monitoring** – by the questionnaire results on the cyber security of transport systems, in 2019–2021, some entities examined did not have a business recovery plan to contend with disaster events, including cyber events. Moreover, many entities examined do not have a testing environment where software and security updates are tested before installation. In addition, a large part of the examined entities is not connected to a specific control system.
-  **Penetration test in transport systems in Municipality A** – as part of the penetration test carried out within the audit's framework, all of the following topics were examined, and deficiencies were found in some of them: user management and permissions; documentation and monitoring; network access control; security of workstations and servers; segmentation and flow control; software updates and security of access to the communication network.



The State Comptroller's Office commends the cooperation of Municipality A in all stages of the penetration test: starting with its planning, through its execution, the process of presenting the findings, the willingness to improve the existing processes, and ending with the rectification of some of the deficiencies found within a short time.

The State Comptroller's Office commends the Ministry of Transport's activity in autonomous vehicles, including the law's amendment, the procedure's publication, and the establishment of the test center in Be'er Sheva. However, the Ministry of Transport has not yet begun conducting audits in this area. In the course of the audit, there was an improvement in several areas operated by the Ministry of Transport's Cyber Division,



including the establishment of sectoral SOCs, the publication of policies, and the performance of audits in some of the supervised entities, to examine their compliance with it.

Key recommendations

-  The National Cyber Directorate should complete the process required to enact the Cyber Law. This issue is relevant to all sectors. Therefore, it is appropriate that the National Cyber Directorate work with the inter-ministerial team to complete the examination of the regulation of the cyber domain and consider introducing across-the-board regulation that will respond to all sectors in the cyber field.
-  It is recommended that the Ministry of Transport amend the laws and regulations and define the priorities for the activity beginning in the field while prioritizing areas where large-scale new projects are established, and areas, where there are many cyber risks and the entities' current state of security does not provide them with an adequate response. It is also appropriate that the Ministry of Transport consider updating the existing concessions, licenses, and engagements and adding to them cyber security requirements, especially those that are expiring soon.
-  It is recommended that the Ministry of Transport, in cooperation with the National Cyber Directorate and the Privacy Security Authority, examine how the relevant information can be transferred between them for concluding events, increasing the resilience of the entities in the sector and improving the guidelines.
-  It is recommended that the Ministry of Transport consider the options for permanently operating SOCs. It is also recommended that the Ministry of Transport examine how to monitor large entities effectively. Given it will take time to connect all entities to the SOC, it is appropriate that the Ministry of Transport prioritize the handling of entities that are not monitored at all.
-  It is recommended that the National Cyber Directorate and the sectoral cyber divisions, including the Ministry of Transport's Cyber Division, bring up every day needs in cyber to prepare templates that can be used by all entities in the sector – among other things, in these fields: recruitment of consultants; procurement of tools; purchase of incident intervention services; establishment and operation of SOC.
-  Given the questionnaire and the penetration test findings regarding cyber security in transport systems, it is recommended that the Ministries of Interior and Transport, in cooperation with the National Cyber Directorate, regulate their responsibilities and establish appropriate procedures. Thus, cyber security in transport systems in the local authorities will receive the appropriate regulatory response. And, a guiding party will



supervise and control the deficiencies rectifying and protecting the systems against cyber-attacks.



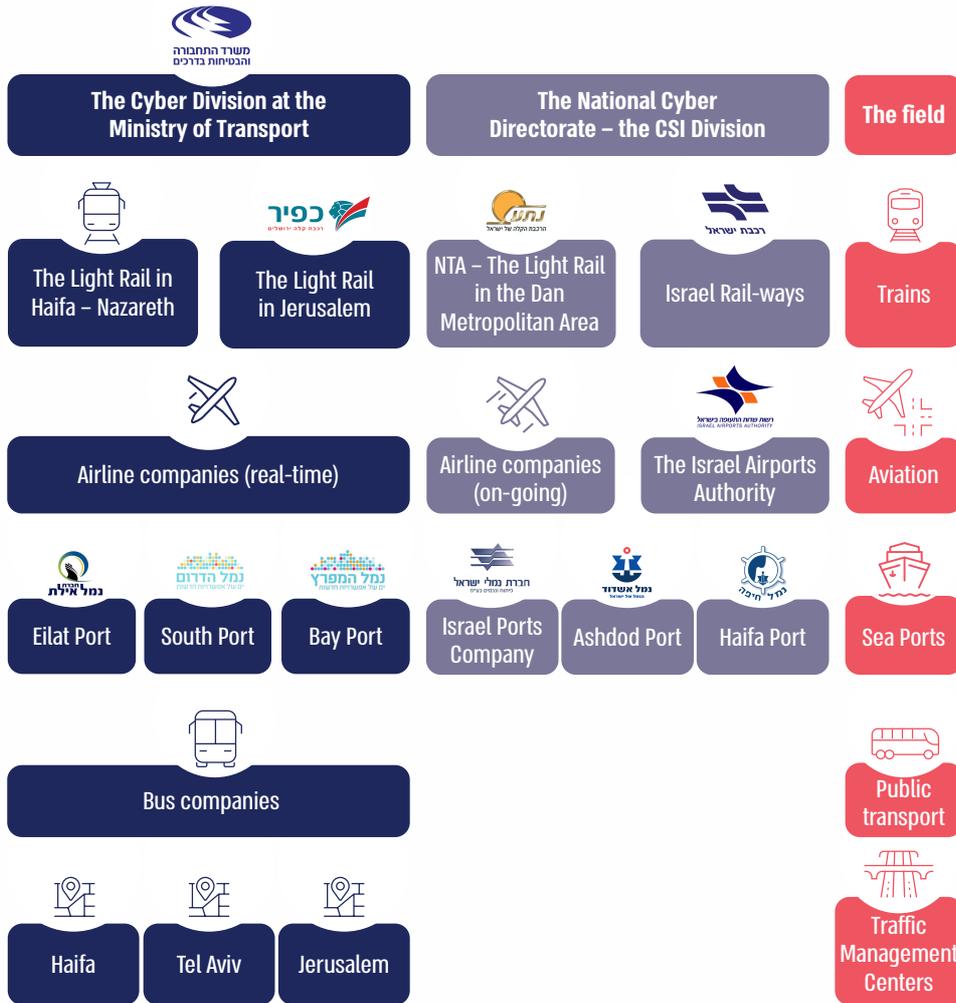
Given the questionnaire findings, the entities examined should evaluate the situation and determine a work plan to rectify the deficiencies. It is recommended that all the authorities where systems in the field of transport are installed conduct risk surveys and penetration tests on their systems and rectify their findings.



It is recommended that Municipality A rectify the deficiencies raised in the transport system's penetration test.



The entities in the transport sector and their regulators in cyber security



The Privacy Protection Authority – Protection of personal information



The state of security in the areas examined in a questionnaire on transport systems

Field	The question	The rate of entities in which a deficiency was found
General	■ writing cyber-related or information security-related requirements in a tender for the selection of the suppliers	High rate
	■ Holding an information-sharing forum with other transport systems	Moderate rate
Corporate governance	■ Conducting penetration tests to detect security vulnerabilities	High rate
	■ Performing risk surveys	High rate
	■ Having a business recovery plan	Moderate rate
	■ Appointing a cybersteering committee	Moderate rate
	■ Appointing officers responsible for cyber protection and information security	Low rate
■ Having backup servers	Low rate	
Architecture and technology	■ Having a testing environment where cyber aspects are examined	High rate
	■ Connection to Information Security System A	High rate
	■ Connection to Information Security System B	High rate
	■ Installing information security updates	Moderate rate
	■ Having an anti-virus	Low rate
	■ Old operating systems	Low rate
	■ Having a firewall	Low rate
Documentation and monitoring	■ Connection to a control center	High rate
	■ Receiving an automatic alert on a specific topic	Low rate
	■ Saving of logs	Low rate
Users and permission management	■ Topic A concerning the management of users and permissions	High rate
	■ Procedure for the removal of users	Moderate rate
	■ A specific control mechanism	Low rate
Remote access	■ Work procedure for remote access of the system suppliers	Moderate rate
	■ Recording or saving the supplier's activity log during a remote connection	Low rate

High rate
 Moderate rate
 Low rate



Summary

The transport infrastructures are designed to ensure the safety and efficiency of sea transport, air transport, and land transport for all road users. The more essential a specific infrastructure is to the residents' day-to-day lives, the more it attracts attackers, and the more it depends on the cyber dimension, the more vulnerable it is to attacks causing operational disruptions and even its complete shutdown, considerable economic damage and harm to human life.

These report findings reflect a fundamental structural and functional problem regarding the State of Israel's preparedness for cyber threats in the transport sector. In the course of the audit, there were improvements in several areas in which the Ministry of Transport's Cyber Division operates, including the establishment of a sectoral SOC to obtain a complete sectoral situation report, enabling the identification of a common denominator during an attack and alerting similar entities against possible exposures, thus helping them to prepare and defend themselves; publishing a policy and conducting audits in some of the supervised entities to examine their compliance with it; promoting the regulation of the autonomous vehicle field, including the amendment of the law, publication of a regulation and the establishment of the trials center in Be'er Sheva. However, there are still some fundamental problems:

There is a lack of regulation concerning the areas of responsibility and authority of the National Cyber Directorate and the Ministry of Transport regarding entities that are not Critical State Infrastructure (CSI); the Ministry of Transport is responsible for the activities of the sector, but it does not have a complete situation report of the levels of security of the entities in it; the lack of consistency between the threats and the responses thereto in the entire sector and the Ministry of Transport's resources; the absence of cyber requirements in engagements in a significant part of the operations in the sector and the lack of allocation of the resources required by the entities for this purpose.

The functional and structural problems this report raises may be relevant to other prominent sectors. Therefore, a systematic approach to these issues may improve the economy's readiness to contend with cyber incidents and that of the significant sectors operating therein.

The audit team performed a penetration test on Municipality A's transport systems. The importance of this innovative process, implemented for the first time by the State Comptroller's Office, is that it allows assessing its actual readiness to face cyber-attacks through the use of tools that reveal security vulnerabilities in its operational work environment and thereby assist practically and accurately to improve the level of security of the audited entities.

The Ministry of Transport and the National Cyber Directorate should ensure that the transport infrastructures, particularly the critical infrastructures, carry out risk assessments regularly and improve their resistance to possible cyber-attacks.



Report of the State Comptroller of Israel | Cyber and
Information Systems | 2022

The Israel Defense Forces

Management of Biometric Information in the IDF and its Cyber Protection



Management of Biometric Information in the IDF and its Cyber Protection

Background

Biometric information is a unique physiological human characteristic that a computer can measure. The risks posed to a biometric database are significant since, unlike other means of authentication such as a certificate, password, or physical means – biometric data cannot be revoked or replaced due to theft or leakage of information.

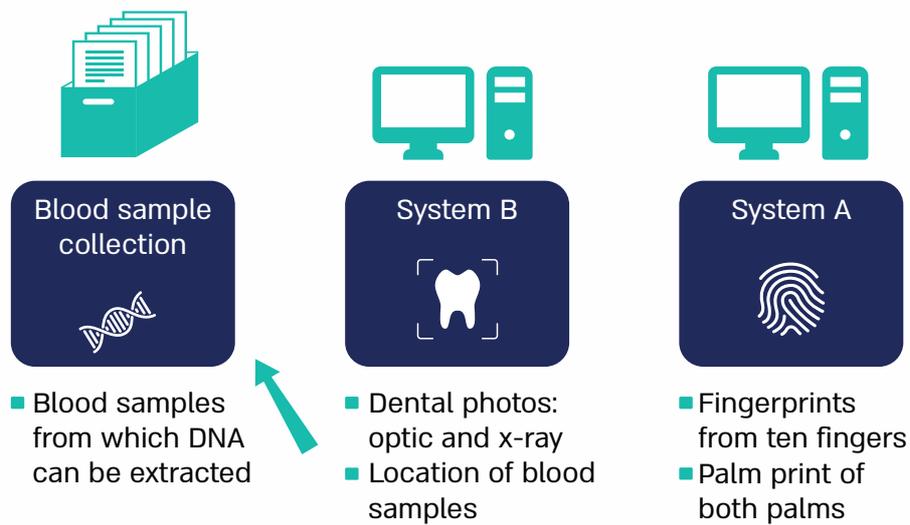
The biometric information the IDF collected from conscripts is used to identify fatalities and is stored in three identification databases (a fingerprints and palm prints database, a dental photographs database, and a blood samples collection). In the acquisition process, as part of the enlistment process, the following means of identification are taken from every soldier enlisting in the IDF: fingerprints and dental photographs. Furthermore, with the conscript's consent, blood samples are taken to produce a DNA sample when necessary. The identification process of fatalities is conducted by comparing the biometric data taken from the conscript to those taken from the fatality.

The IDF should act under its cyber security policy, the Protection of Privacy Law, 1981, and the Protection of Privacy (Data Security) Regulations, 2017 (Data Security Regulations). According to the Data Security Regulations, a database containing biometric information and over 100,000 records is required to meet a high level of security. The Regulations detail how the level of security settings for the database should be maintained.

The IDF has three critical information systems to manage the identification process: System A and System B, which manage the identification database, have been classified by the IDF and are required to meet a high level of security under the Data Security Regulations. System C manages the records of the fatality, including its identification process. The Weapons Officer at the Chief Personnel Officer Headquarters in the Personnel Directorate is the project manager of the identification systems and is responsible for formulating the systems' cyber security response. The 'Tachlit' branch in the 'Shahar' Unit is responsible for developing and maintaining the systems. The primary systems users are the 'Meitav' Unit (in the acquisition process) and the Identification and Burial Branch in the Military Rabbinate (in the fatality identification process).



Following is a diagram presenting the means of identification and the information stored therein:



Key figures

3 information systems

manage the means of identification

hundreds of thousands

of fingerprint records are kept in the IDF identification database

7 years

have passed since the IDF's cyber security policy was updated

26 years

in which the privacy protection General Staff directives were not updated. Thus, they do not refer to the 2017 Data Security Regulations

0

number of risk surveys and penetration tests conducted to examine the protection level of the identification systems since their establishment in 2005–2006 (about 16 years ago)

50%

2 of the 4 acquisition stations for collecting photographs of the oral cavity in the enlistment process are shut down from August 2021 (more than six months)

95%

of the dental photographs found in the identification database were of insufficient quality

1 of every 87

of those currently serving in mandatory service and standing army officers (1.15%) allowed only one capability mean, raising concerns about their identification in the future



Audit actions



From August 2021 to April 2022, the State Comptroller's Office audited the "Biometric Information Management in the IDF and its Cyber Protection". The audit was conducted in the IDF: in the Personnel Directorate – at the Strategy, Digital and Systems Branch (ADAM) and in the Headquarters of the Chief Personnel Officer; in the intake and sorting section – at the Meitav Unit; in the Shahar unit – at the Tachlit branch; in the Military Rabbinate – at the Identification and Burial Branch. Completion examinations were conducted at association A and the Privacy Protection Authority at the Ministry of Justice.

This report was submitted to the Prime Minister on July 31, 2022, and was classified as confidential until its discussion at the State Audit Committee's Subcommittee.

Under the authority vested upon the State Comptroller in Section 17(c) of the State Comptroller's Law, 1958 [Consolidated Version], considering the government's reasoning, consulting with the bodies entrusted with the security of defense information, in coordination with the Knesset chairman, and as the said subcommittee did not convene, it was decided to publish this report while classifying as confidential parts thereof. These sections will not be brought before the Knesset and will not be published.

The audit report's findings and recommendations are correct as of the aforementioned date of its publication.

Key findings



The cyber security policy – the IDF's cyber security policy includes part of the topics that the Government's Cyber protection Unit (YAHAV) defined as mandatory in the security policy such as protection of records, logical and physical protection, and the organizational structure, but does not include management and classification of assets, the supply chain, human resources and compliance with legal requirements (such as Data Security Regulations). Furthermore, the cyber security policy has not been updated since April 2015, for seven years, during which there have been technological changes and changes in the obligations applicable to the IDF on information security under the Protection of Privacy (Data Security) Regulations from 2017.



The cyber security response – System A and System B were classified with moderate security even though these systems are required to meet a high level of security under the Data Security Regulations, and despite the significant damage that may be caused by the leakage of sensitive biometric information stored in these systems. Moreover, the



IDF's identification systems do not have a detailed documented cyber-security protection response, including the specific protection requirements for these systems according to their classification.

-  **Information security officer** – the IDF has several entities dealing with various aspects of information security of information systems, including the Cyber Protection Unit at the Center of Computing and Information Systems (Mamram), the Information Security Department (Mahbam), the Weapons Officer and cyber-security policy officials in the Computer and IT Directorate. However, it has no single entity responsible for all the information security aspects of the identification systems which his role and areas of responsibility were defined under Regulation 3 of the Data Security Regulations and the IDF cyber security policy.
-  **Compliance with Data Security Regulations** – the Personnel Directorate has no regular monitoring plan to evaluate the degree of the identification databases' compliance with the Data Security Regulations requirements, and no audits were carried out on these issues. It was also found that the General Staff directives on privacy protection have not been updated since they were written in 1996 (26 years ago). Therefore, they do not refer to the Data Security Regulations published in 2017. Moreover, the Privacy Protection Authority did not conduct audits and organization-wide supervision on the IDF databases in general and the biometric databases for identifying fatalities in particular, to ensure that the databases comply with the Data Security Regulations even though the IDF maintains databases containing sensitive and personal information about many citizens.
-  **Database definitions document** – the IDF did not formulate a definition document for the identification databases as required by the Data Security Regulations, including essential information about the databases and their purpose, such as detailing the main risks of harm to information security and contending with them.
-  **Superfluous information** – the IDF did not examine whether superfluous information was kept in the identification databases once a year, as required by the Regulations. The identification databases contain superfluous information, like biometric information of soldiers who passed away (deceased) and for whom no identification process was carried out. Biometric information of deceased persons may be more easily used for impersonation and identity theft since no one will complain about the use thereof.
-  **Physical protection** – the IDF did not formulate a dedicated physical security procedure for the identification systems as required by Regulation 4 of the Data Security Regulations, even though they store biometric, personal, and sensitive information requiring a high level of security. Disparities were also found in the physical security of the systems in Unit A as follows: physical protection and control of the entrances and exits, protection of the work environment, and environmental protection.



-  **Logical protection** – disparities were found at the level of logical protection in the following topics: authentication; access rights; access control survey; control over the execution of unauthorized operations; encryption mechanisms; and regular control for application protection processes.
-  **Business continuity** – the IDF did not develop a business continuity plan for the identification process that covers all the identification means processes and all the units involved in them, and it did not define which parts of the process are critical during an emergency incident. Furthermore, it did not conduct an emergency operation drill of the entire array required to identify a fatality. In addition, the following disparities were found: the IDF did not ensure that the systems were regularly accessible from alternate sites determined in advance; in the MAMRAM unit, no periodic drills were carried out to do a backup checkup to ensure their integrity and compliance with the data recovery; the physical collection of blood samples is kept in a single location, and there is no redundancy for the information therein by storing them in a different location.
-  **Integrity of the means of identification** – the IDF's biometric database containing hundreds of thousands of records is incomplete. The database contains several tens of thousands of records of mandatory service soldiers and standing army officers, which as of the audit completion in April 2022, lack the following means of identification: 0.5% of the fingerprints, 6.6% of the X-ray photographs, 32.8% of the oral cavity photographs and 3.8% of the DNA samples. Also missing are hundreds of fingerprints of soldiers who enlisted in 2016 and 2017 and several thousand dental photographs of standing army officers who enlisted in 1994–2004. In addition, by the Medical Identification Section audits it carried out in 2018–2019 about 95% of the dental and oral cavity photographs are of insufficient quality. The poor acquisition quality of the dental photographs was still not addressed by the audit completion in April 2022.
-  **Methodology for project management** – the methodology for project management in the IDF (Personnel Directorate Standing Order (PDSO) 10/1) published by the Planning Division is not specific to manage information systems projects and therefore does not include a detailed reference to mandatory issues that are required in accepted methodologies for the management of information systems projects. In addition, the methodology does not include tools that will help the entities in its implementation: standards, guidelines, working procedures, and uniform templates in project management. Moreover, the methodology does not address project management according to the "agile"¹ method, even though the IDF develops systems according to this methodology, for example, the new B System.
-  **Project management** – in the identification systems, no fundamental documents such as detailed requirements documents or intermediate products as required in work processes according to accepted methodologies for managing information systems

1 (In Hebrew) The amalgamation of the words "nimble" and "flexible".



projects and according to PDSO 10/1. Without these essential documents and intermediate products, there is a risk that the developed systems do not suit the users' requirements.

 **Project manager** – the identification systems were not managed according to accepted methodologies for project management; this includes gaps found in the following matters, under the purview of a project manager: preparation of work plans and the monitoring of their execution, client management and participation, bringing the projects up for discussion at steering committees meetings, risk management, change management, and bag management.

 **Identification of fatalities during a mixed mass fatality disaster (MFD) involving civilians and soldiers** – the use of the Center for the Collection of Fatality Data ("Ha'Tzvi Center") of the Military Rabbinate during a mixed MFD involving civilians and soldiers was not regulated. Furthermore, although the IDF maintains a database containing hundreds of thousands of records of civilians and soldiers, including unique means of identification such as fingerprints and palm prints, the possibility of using the identification databases held by the IDF for identifying victims during an MFD has not been thoroughly examined.



Increasing the IDF's work interfaces with the Privacy Protection Authority – in 2021, the IDF, in cooperation with the Privacy Protection Authority, began formulating a comprehensive work plan that will address the following: appointment of a Privacy Protection Officer in the various units, internal IDF informational activities to strengthen its privacy protection, the inclusion of the privacy protection in the audit carried out by the Personnel Directorate and amending the General Staff directives.

Outsourcing – during the audit, the IDF ensured that Company B, which provides technical support to System A, had secure access to the identification systems and audited this access.

Completing insufficiencies in means of identification – between the recruitments from February to March 2022, the IDF began acquiring identification means from the fighters using a mobile station with acquisition stations borrowed from the enlistment process.



Key recommendations

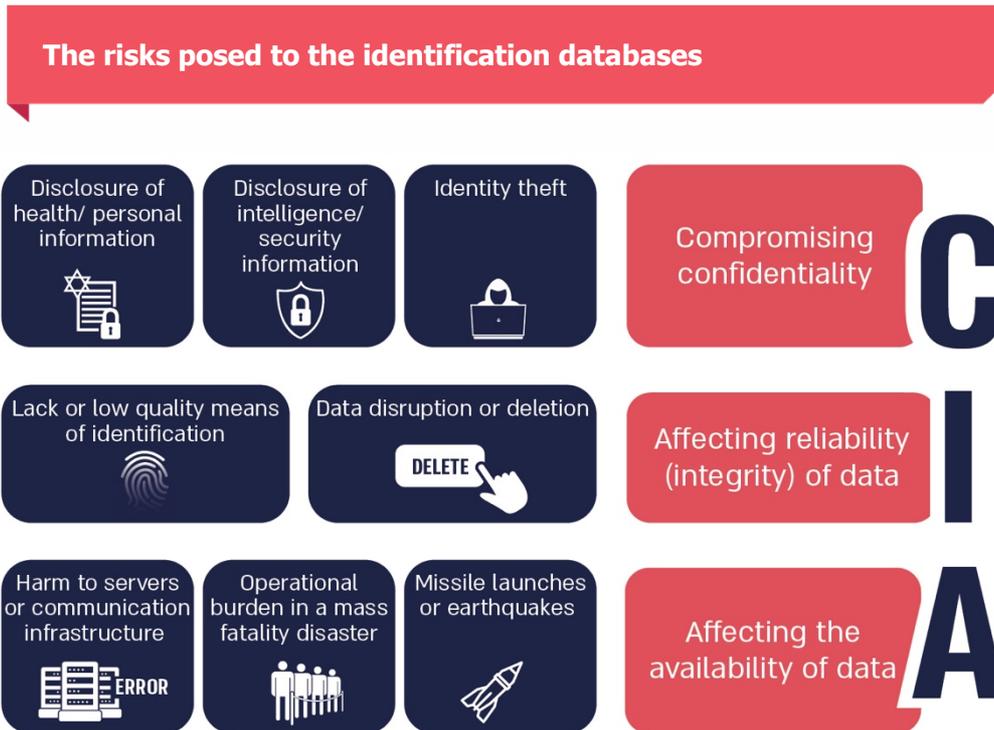
-  It is recommended that the Biometric Applications Officer presents to the IDF the regulatory document he drew up in December 2015 with the IDF Information Security Department (Mahbam) and examine together the need to update it according to the work format established with similar special bodies.
-  It is recommended that the Cipher and Security Center in the protection Division update the cyber-security policy and include the issues specified in accepted cyber-security policy such as the Government's Cyber protection Unit (YAHAV) directive on policy. It should update it periodically according to the technological changes and risks in the field, and meet the relevant requirements of the law and Regulations.
-  It is recommended that the Information Security Department periodically re-examine and validate the classification of the identification systems considering the current risks posed to the information stored in these databases and the risks due to an information leak. The Chief Personnel Officer Headquarters in the Personnel Directorate should ensure that the principles of the cyber security-policy are anchored in a cyber-security response document and implemented in the identification systems in stages of development and maintenance. In addition, it is recommended that the Chief Personnel Officer Headquarters in the Personnel Directorate verify every year that the systems' cyber-security response adequately contends with the risks faced at that time and with the current threat scenarios.
-  It is recommended that the IDF appoint an Information Security Officer responsible for the identification systems under the Protection of Privacy Law and Data Security Regulations.
-  The Personnel Directorate should prepare an ongoing control plan for the databases' degree of compliance with the Data Security Regulations and verify its execution once every two years or as part of a risk survey. It is further recommended that the Personnel Directorate, in cooperation with the Computer and IT Directorate, update the General Staff directives on privacy protection.
-  It is recommended that concurrently with the ongoing legislative amendment process, the Privacy Protection Authority will regulate the ability to supervise and enforce the information databases in the IDF, including the identification databases. It is also recommended that the Personnel Directorate, in cooperation with the Privacy Protection Authority, implement the work plan formulated following the meeting in May 2021, including promoting training in the IDF on compliance with Data Security Regulations and formulate a plan for training officials to serve as internal supervisors within the IDF.



-  The IDF should write a physical security procedure under the Data Security Regulations. Furthermore, Unit A, in cooperation with the IDF's information security officials, should protect the compound that was examined in the audit.
-  It is recommended that the Information Security Officer, in cooperation with the IDF Information Security Department (Mahbam), reduce the gaps in logical protection.
-  It is recommended that the IDF formulate a business recovery plan for the identification process, examine the entirety of the processes, the risks, and the consequences of their realization, and define the level of response given to each risk. It is also recommended that the IDF periodically conduct emergency drills covering all processes of identification means and the units involved in these processes.
-  It is recommended that the Personnel Directorate reduce the disparities in the acquisition of the missing identification means, prioritize its completions according to the nature of the soldiers' service (combat service, risk levels, etc.), the type of identification means (fingerprints) and the number of times they were called for completion. In addition, operate a mobile station to acquire identification means, including dental photographs.
-  It is recommended that the Personnel Directorate, in collaboration with the Planning Division, update the relevant procedures for managing information systems projects (10/01 and 10/6) so they include a detailed reference to the mandatory issues required in accepted methodologies for managing information systems projects and adapt the methodology for project management using the "agile" method. It is further recommended to form implementation tools of the methodology and establish a supporting body for project management (such as a PMO) to contend with this need.
-  It is recommended that the Chief Personnel Officer Headquarters in the Personnel Directorate manage the identification systems according to accepted methodologies for managing information systems projects and to PDSO 10/1 and formulate the required work documents according to these methodologies. The Personnel Directorate should formulate an orderly plan defining the areas of responsibility of the Chief Personnel Officer Headquarters in the Personnel Directorate as the project manager of the identification systems in preparation for the next steps in the development of these systems and that it implements it according to accepted methodologies.
-  It is recommended that the National Emergency Management Authority (NEMA), in cooperation with the Authority for Evacuation, Relief, and Treatment of Victims in an Emergency, examine the existing response and the necessary response to identifying victims during a mass fatality disaster (MFD), regulate the division of responsibilities between the different bodies and promote the use of Ha'Tzvi Center as a national fatality concentration station during a mass fatality disaster. In this framework, it is recommended to examine the feasibility of using the IDF's database and other databases to identify fatalities during a mass fatality disaster. It is recommended that the matter be examined in cooperation with the representatives of the Privacy Protection Authority



and representatives of the IDF: the Personnel Directorate, the Military Rabbinate, and representatives of the Military Advocate General's Office.





The identification databases' compliance with the Data Security Regulations requirements

Regulation	Topic	The audit findings
2	Database definitions document	Non-existent
3	Information security officer	Not appointed
4	Security procedure	Non-existent
5	Mapping of the database systems and the performance of a risk survey	Partially found
6	Physical and environmental security	Partially found
7	Information security in personnel management	Partially found
8	Access authorization management	Partially found
9	Identification and verification	Partially found
10	Access control and documentation	Partially found
11	Documentation of security incidents	Partially found
12	Mobile devices	Found
13	Secure an updated management of the database systems	Partially found
14	Communications security	Found
15	Outsourcing	Found
16	Periodic audits	Non-existent



Summary

The IDF manages identification information systems identifying fatalities. These are systems managing biometric databases including medical, personal, and sensitive information. Therefore, it is required that the security level of the databases be high under Data Security Regulations.

The findings of this report present significant information security gaps found in these sensitive systems, and indicate non-compliance with some Data Security Regulations and non-implementation of requirements included in the cyber-security policy documents. This state of affairs creates a risk of damage to the reliability, integrity, availability, and confidentiality of the information in the databases.

The report includes additional findings on the operation and management procedures of the identification information systems. Among other things, it was found that the information systems are not managed efficiently and according to an orderly methodology for managing information systems projects, resulting in the concern that the identification systems will not be able to fulfill their purpose. It was also found that the project manager needed to prepare work plans for the identification systems and ensure that the establishment and management of the systems met the accepted goals of content, schedules, costs, and customer satisfaction.

The head of the Personnel Directorate should rectify the deficiencies and examine the recommendations in this report.



Report of the State Comptroller of Israel | Cyber and
Information Systems | 2022

The Israel Tax Authority

Establishing a New Foreign Trade System at the Tax Authority – the "Global Gateway" Project



Establishing a New Foreign Trade System at the Tax Authority – the "Global Gateway" Project

Background

Increased international trade (import and export) in goods and services manifests the globalization process. The "Global gateway" project establishes a new computer system in the Customs Administration at the Israel Tax Authority to manage the State of Israel's foreign trade, including the rapid transit of goods to and from the country. The project is outsourced to an external supplier (Company A). It began in 2008, and there have been many delays over the years. At the audit completion, phases A, B, and C of the project (in imports) went live. The project's final phase – phase D (export) – is to be completed in 2023.



Key figures

**NIS 240
and 172
billion**

import and export of goods to and from Israel, respectively, in 2020, according to the Central Bureau of Statistics data

12 years

the delay time of the project's planned end date compared to the date stipulated in the original agreement¹. The project is expected to take 15 years – 5 times longer than the original plan

**NIS 94
million**

the system's development costs increase due to delays in the project until the launch date of phase B – a deviation of 67% of the cost according to the original agreement

**NIS 627
million**

sum increase in the Tax Authority's contract with Company A (for development and maintenance)² compared to the original agreement

NIS 1 billion

total sum approved engagements with Company A. 62% was approved through exemption from a tender

48 years

the cumulative contract period with Company A for the development and maintenance of the Global Gateway system and the old system, from 1991 to 2039³

57 million

number of messages that went through the Global Gateway system in November 2021 ("online shopping month")

**6.7
million**

number of import declarations that went through the system in November 2021 in cargo release procedures from customs

- 1 According to the original agreement between the Tax Authority and Company A from 2008, the project was planned to be completed three years later – in 2011.
- 2 For the development of the Global Gateway System and its maintenance as well as for extending the maintenance of the old system or parts thereof, due to the delays in the project.
- 3 Including option of six years.



Audit actions

 From May 2021 to March 2022, the State Comptroller's Office examined the Global Gateway project, including the delays in the project schedule, the contracts with Company A, the users satisfaction of the system, and information security. The audit was conducted at the Israel Tax Authority ("Tax Authority" or the "Authority"). Completion examinations were done at the National Digital Agency at the Ministry of Economy and Industry ("Digital Agency") as well as at the National Cyber Directorate at the Prime Minister's Office (the "Cyber Directorate"). Moreover, this report examined the actions taken by the Customs Administration at the Tax Authority to rectify deficiencies raised in a previous audit report published by the State Comptroller on the project in 2016⁴ (the previous audit report).

The report was submitted to the Prime Minister on July 31, 2022, and was classified as confidential until its discussion at the State Audit Committee's Subcommittee. Under the authority vested upon the State Comptroller in Section 17(c) of the State Comptroller's Law, 1958 [Consolidated Version], considering the government's reasoning, consulting with the bodies entrusted with the security of defense information, in coordination with the Knesset chairman, and as the said subcommittee did not convene, it was decided to publish this report while classifying as confidential parts thereof. These sections will not be brought before the Knesset and will not be published. The audit report's findings and recommendations are correct as of the aforementioned date of its publication.

Key findings

 **Delays in the completion of the project** – according to the original agreement with Company A from 2008, the project's completion was planned for three years later – in 2011. However, along the way, there were many difficulties in its advancement, and as a result, the project is expected to end with considerable delay and take 15 years (5 times longer than as planned). Phase B went live in 2018, while phase D is scheduled for completion in 2023. Some of the reasons for the delays are: the system's lack of readiness in terms of content; system malfunctions; multiple change requests; Tax

4 The State Comptroller, Annual Report 67A (2016), "The Global Gateway Project for the Establishment of a New Foreign Trade System at the Tax Authority", pp. 303–355.



Authority employees' sanctions; and the degree of cooperation of the foreign trade community⁵.

-  **Increase in the system's development cost** – due to the delays until the launch date of phase B – in January 2018, the development cost of the system increased from NIS 140 million (the cost in the original agreement) to NIS 234 million – a 67% deviation. Furthermore, the delays in the project left the system with ineffective processing procedures. They delayed the realization of the supposed economic benefits from the system, which were the project basis, including reducing trade costs and rapid movement of goods to and from the country, increasing enforcement, and improving the service to the citizens.
-  **Increase in engagements in the project** – in addition to the increase in the system's development cost, the delays in the project necessitated repeated extensions of the old system maintenance engagement. As a result, the total sum of the engagement with Company A increased from NIS 384 million (the sum in the original agreement) to approximately NIS 1 billion – an increase of NIS 627 million (163%); and the engagement period with Company A increased by 15 years: from 16 years in the original agreement to 31 years.
-  **Exemption from tender in engagements** – 62% of the engagement sum with company A (NIS 627 million) and half of the engagement period with it (15 years) was approved through an exemption from tender (continuing engagement) – which is not the preferred method under the Mandatory Tenders Regulations, 1993. The changes approved in this method constitute a considerable deviation from the planned outline of the project, given the need to extend the validity of the original maintenance agreement by many years.
-  **The engagement with Company A** – by a systemic issue raised in the previous audit report, Company A is responsible for both the maintenance of the old system and for the development of the new system and its maintenance, thus creating a situation of "captive supplier-customer relations" and "supplier with a dual personality". This situation in the project is expected to continue until its conclusion⁶.
-  **The total duration of the engagement with Company A and its scope** – due to the lack of competition in the tender from 2004 and the delays in the project, the cumulative engagement between the Tax Authority with Company A regarding the two

5 The system serves all the parties involved in the foreign trade processes of the State of Israel, including customs agents and importers.

6 When phase D goes live, the maintenance of the old system will be suspended.



systems (the Global Gateway system and the old system) will last 48 years (from 1991 to 2039⁷) and the financial scope will exceed NIS 1 billion.

-  **Extension agreement for the project** – although the engagement time between the parties, according to the expansion agreement, ended in January 2020, in May 2022, the parties have not yet signed an extension agreement. Hence, for more than two years, the Tax Authority continued to purchase services from Company A, for about NIS 74 million⁸, without a validly signed engagement agreement.
-  **Convening of the Steering Committee** – in 2019–2021 there were significant delays in the project, its completion date was postponed by three years and the engagement budget increased by NIS 106 million. Nevertheless the Tax Authority convened the steering committee once a year (in 2020) or twice a year (in 2019 and 2021) in contravention of its decision to convene every quarter.
-  **Service Level Agreement (SLA)** – four years after phase B (the primary phase) went live, the determining procedure of the service level indices to measure the system was not completed, and at the audit completion, an updated service level agreement had not yet been signed between the parties. Moreover, the satisfaction degree of the system users with the level of service provided to them through the support center operated by Company A was not examined.
-  **Internal users' survey** – the Tax Authority conducted the first satisfaction survey among internal users in January 2021 – three years after the launch of phase B. A third of the respondents (16 out of 52) were marginally or not at all satisfied with the display of the system screens, and a quarter of them (13 out of 52) felt the same concerning the system search screens. In another survey conducted by the Authority during the audit in November 2021, 37% of the respondents (21 out of 57) stated that there is a great, and a great extent, lack of training on the system.
-  **External users' survey** – a satisfaction survey for the external users was also conducted three years after the launch of phase B in February 2021. Only online users of the Global Gateway participated in the survey, and it did not include the external users working in the system. Most respondents to the survey rated the system's performance as average or less in response speed (51%) and in the user experience (57%).
-  **Information security in the system** – the project was managed for over a decade without completing the necessary response for information security, focusing on updating the requirements defined in the past. In the time (14 years) from the information security requirements characterization in the tender in 2004 to the

7 Including the six option years (2033–2039).

8 For monthly maintenance for NIS 2.6 million from January 2020 to May 2022 (including VAT).



implementation of the system in 2018, inconsistencies were created in the system information security. Following the conclusions from information security events in the Israeli economy in 2019 and their possible impact on Customs, a multi-year work plan was formulated. The audit found that the Tax Authority is working on implementing the plan.

 **Cyber protection in the supply chain** – company A is a significant factor in the Global Gateway system and its operation. Therefore, a cyber-breach in the company might cause damage to the system. Despite this, at the audit completion, Customs did not know whether Company A had completed the planned examination procedure of the level of cyber protection in the 'Yuval' system (goals and controls for organizations)⁹, and it did not have the results document of the said examination. Furthermore, Customs did not complete the examination of the level of cyber protection in the 'Yuval' system of suppliers providing it with computing and communication services defined as "material suppliers," which have been associated with the Global Gateway system for some time. It should be noted that after the audit completion, the Cyber Directorate published an updated directive in which the timetables for this examination were postponed.



Since launching phase B (import), the Global Gateway system has contributed significantly to streamlining import processes and improving Customs' ability to perform a risk assessment and enforce trade laws. This is through managing work processes in a computerized manner, switching to paperless work, and using advanced analytical tools.

Key recommendations

 It is recommended that the Tax Authority and the Digital Agency examine the significance of engagements with one supplier for 48 years in a sum exceeding NIS 1 billion. In this context, it is proposed to encourage competition in large government IT (Information technology) tenders, such as reducing entry barriers in tenders and splitting the service into several parts, preserving knowledge in the government body, and limiting the duration of the engagement to encourage more suppliers to submit bids in tenders and to encourage technological innovation. Such an examination is necessary to analyze, learn, and generate systemic insights, both in managing large government software development projects and government IT engagements.

 It is proposed that the Digital Agency consider examining and mapping the existing government IT engagements, including collecting data on their duration, financial scope,

9 A system for managing cyber risks and information security developed by the Cyber Directorate.

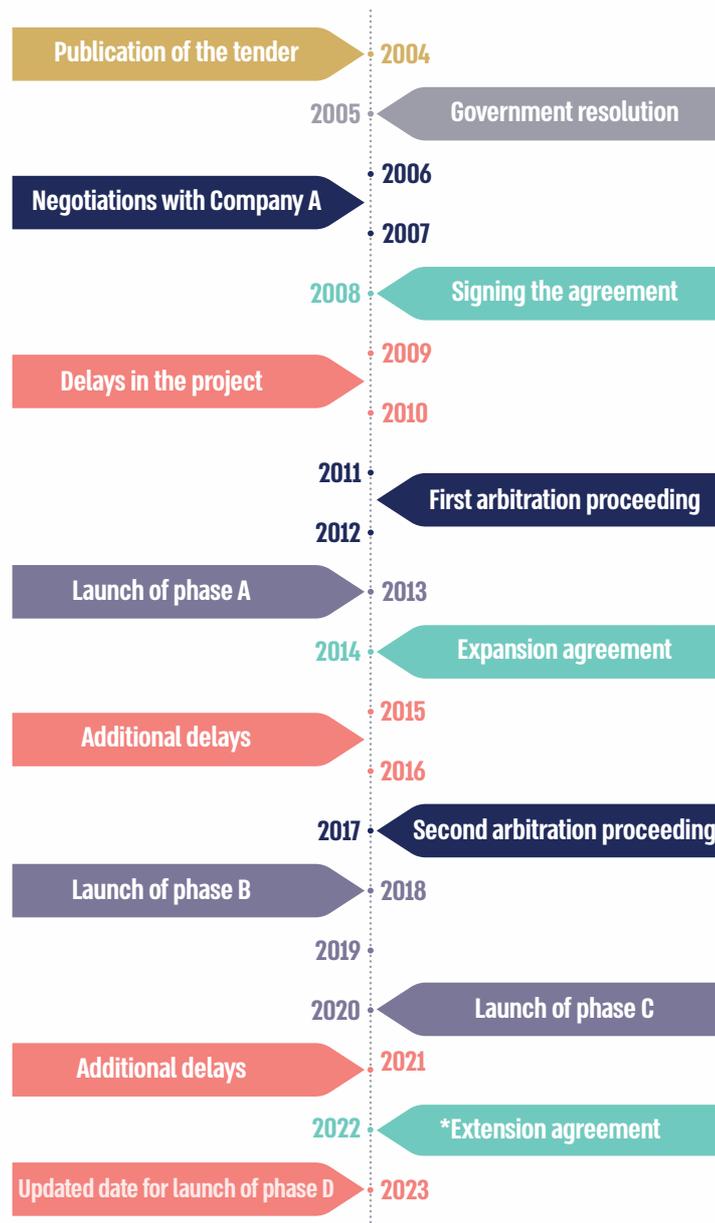


and approval method (through a tender process or exemption from a tender). This will enable identifying fundamental problems in government IT engagements and examination of aspects of the concentration of suppliers in this field, including situations of a "supplier with a dual personality" and "captive supplier-customer relationships".

-  The Tax Authority should sign an updated extension agreement with Company A, including all the required annexes, an updated work plan defining agreed schedules, and a dispute resolution mechanism. Furthermore, the Tax Authority Director should ensure that the Steering Committee, the guiding body and ultimate auditor of the project, would convene every quarter, as it has stipulated, to monitor and control the project until all system components go live and the project's goals are completed.
-  The Tax Authority should determine the agreed service level indices (SLA) and formulate a final version of the agreement to control and monitor Company A's compliance with the required service level. Moreover, since in the two surveys conducted by Customs among the internal users in 2021, dissatisfaction with the display mode and the screen colors came up repeatedly, it is recommended that Customs complete its handling of the matter. It is recommended that the Authority conduct an extensive satisfaction survey among all external users who work with the system with high frequency and daily, including customs agents, forwarders, and importers. Such a survey will enable receiving feedback on the work scope of the external parties in the system and its processes; collecting information about difficulties and problems to learn and implement and drawing lessons for the launch of the export phase.
-  The Tax Authority and the Cyber Directorate should ensure the completion of all information security gaps that arise within the Cyber Directorate's guidance procedure and monitor the implementation of the requirements for information security in the system on an ongoing basis. Customs should verify that Company A has completed the examination of the 'Yuval' (goals and controls for organizations) cyber-system protection level and that it regularly performs tests of its protection level, receive the results of the tests, and follow the rectifying of the gaps that arise in these inspections. Customs should also ensure the examination completion of the level of cyber protection in the 'Yuval' system of the suppliers associated with the Global Gateway system which were defined as "material suppliers," according to the Cyber Directorate's instructions. If Customs cannot coordinate with the companies in the execution of the inspection, it should regulate compensatory controls to protect the system.



The sequence of events in the Global Gateway project, 2004–2022



According to the data Tax Authority, processed by the State Comptroller's Office.

* At audit completion, this agreement had not yet been signed.



Users of the Global Gateway system



According to the data Tax Authority, processed by the State Comptroller's Office.

* At audit completion, this agreement had not yet been signed.



Summary

The Global Gateway project to establish a new foreign trade system is a complex project of national importance. The system serves about 1,200 internal users at the Tax Authority and over 1,500 external parties in the foreign trade community. It is designed to optimize and improve the service along the supply chain of an import-export transaction and increase the enforcement of trade laws. The system is a significant component in managing Israel's foreign trade. Implementing the import phase in the system in 2018 considerably, streamline the import work procedures through their computerized management and reduce the need to attend the Customs sites for service physically.

Over the years, the many difficulties in the project led to two arbitration proceedings and many delays. They even delayed the realization of the economic benefits of the system, including the reduction of trade costs, the rapid movement of goods, to the country and from it, and the improvement of service to the citizen. Because of these delays, the Tax Authority was repeatedly required to extend the engagement period with Company A and to increase the engagement sum by hundreds of percent. All this under the exemption from tender, which is given in a situation where there is a considerable deviation from the project's budget and a delay of over a decade in its completion. Throughout the project years, Company A was responsible for both the old system's maintenance and the new system's development and maintenance, thus creating a situation of "captive supplier-customer relations" and "supplier with a dual personality".

It is recommended that the Tax Authority complete the system according to the schedules it determined, improve the areas where dissatisfaction arose among the system users, and ensure that the supplier meets the level of service according to the indices examined. Moreover, given the increasing threats in cyber protection to critical systems in the government and the project's outsourcing, the Authority should lead and plan the system's cyber protection and find solutions for all its current information security needs.

Due to the delays in the project and the lack of competition in the 2004 tender, the cumulative engagement period between the Tax Authority and Company A regarding the two systems will last 48 years, and the financial scope will exceed NIS 1 billion. It is recommended that the Tax Authority and the Digital Agency examine the significance of a multi-year engagement with one supplier. It is further proposed to encourage competition in large IT tenders in the government and preserve knowledge in the government body. It is also recommended that the Digital Agency continue to conclude from this project to incorporate them into projects of a similar scope in the government system and consider mapping government IT engagements. Such an examination is necessary to identify fundamental problems and generate systemic insights in managing large software development projects in the government and in government IT engagements.



Report of the State Comptroller of Israel | Cyber and
Information Systems | 2022

The Government Water and Sewage
Authority

Regulation and Supervision of Local Water Suppliers in Cyber Protection



Regulation and Supervision of Local Water Suppliers in Cyber Protection

Background

Cyberspace includes computers, automated systems, networks, software, computerized information, digital content, traffic, and control data. A cyber-attack is a sequence of actions carried out by an adversary in cyberspace. Cyber threats are intensifying with the growth of cyberspace and might lead to damage both within and in the physical space such as desalination plants, water suppliers, and infrastructure. According to Water Authority documents, there has been an exacerbation of cyber threats to the computer systems of Israel's water and sewage sector in recent years. Cyber protection is crucial for all parties in the water sector, including its many suppliers.

Key figures

a gap

in the workforce headcount in the sectoral unit at the Water Authority compared to the headcount standard according to the draft standard for the sectoral unit compiled by the National Cyber Directorate (NCD)

part

of all the water suppliers that, in the opinion of the Water Authority, should be connected, were connected to the Ministry of Energy's Cybernetic Center by May 2022

part

of the water corporations examined by the Water Authority in 2021 reached a low score for their cyber-attacks preparedness

Audit actions

 From June to December 2021, the State Comptroller's Office examined the regulation and supervision of the local water suppliers in cyber protection. The examinations were conducted at the Water Authority and the National Cyber Directorate (NCD). Completion examinations were conducted at the Ministry of Energy and Mekorot (Israel national water company).



This report was submitted to the Prime Minister on July 31, 2022, and was classified as confidential until its discussion at the State Audit Committee's Subcommittee.

Under the authority vested upon the State Comptroller in Section 17(c) of the State Comptroller's Law, 1958 [Consolidated Version], considering the government's reasoning, consulting with the bodies entrusted with the security of defense information, in coordination with the Knesset chairman, and as the said subcommittee did not convene, it was decided to publish this report while classifying as confidential parts thereof. These sections will not be brought before the Knesset and will not be published.

The audit report's findings and recommendations are correct as of the aforementioned date of its publication.

Key findings

-  **Definition of critical state infrastructure bodies (CSIs) in the water sector** – Mekorot is the only CSI body in the water sector, and the NCD directly supervises it. The other bodies in the water sector are under sectoral supervision. Defining additional large infrastructure bodies in the water sector has not yet been examined and discussed by the dedicated steering committee.
-  **Regulation of water security rules** – at the audit completion in December 2021, the Water Authority Council did not regulate rules under Section 18A of the Water Law addressing the water suppliers' obligation to operate a monitoring and control system and a protection system against cyber incidents. Their obligations are to submit an information security plan for approval by the Water Authority, and to connect their computer systems to the Cybernetic Center. In addition, the authority of the director of the Water Authority's sectoral unit to instruct the water suppliers was not regulated, and neither was the authority of the suppliers to abide by them. The regulation proposal above was stipulated in the Water Rules (Water Damage Event), 2022 draft, which the Authority's council discussed in January 2022.
-  **The sectoral unit at the Water Authority** – at the audit completion, December 2021, the National Cyber Directorate did not set a headcount standard for a sectoral unit at the Water Authority. A discrepancy was found in the headcount standard in the sectoral unit at the Water Authority compared to standard for the sectoral unit draft compiled by the NCD. Additionally, until the audit completion, outsourced workers have staffed all jobs not standardized in the sectoral unit at the Water Authority.



-  **Penetration tests** – inconsistencies were found in this area.
-  **Connecting the water suppliers to the Cybernetic Center (CC) of the Ministry of Energy** – only a part of all the water suppliers that according to the Water Authority should be connected was connected to the Ministry of Energy's CC by May 2022.
-  **Preparedness for cyber protection among the water and sewage corporations** – in recent years and until the audit completion, the Water Authority conducted cyber audits of some corporations. Some water corporations examined by the Water Authority in 2021 reached a low score for their cyber protection readiness.



Establishment of the Cybernetic Center (CC) – the Ministry of Energy established a Cybernetic Center that monitors all energy infrastructures, integrates information received from them, and provides a situation report on the cyber protection of the energy sector.

Key recommendations

-  It is recommended that the NCD examine the latest data of the significant and key water and sewage sector entities from time to time to determine which should be discussed in the dedicated steering committee.
-  It is recommended that the Authority Council and the Water Authority regulate the water suppliers' obligation to operate monitor and control system and a cyber incident protection system, to prepare information security plans, and to anchor in water safety rules the authority of the Water Authority to instruct the water suppliers in the cyber field.
-  It is recommended that the National Cyber Directorate complete the procedure for determining the headcount standard required in the cyber sectoral unit at the Water Authority.
-  It is recommended that the Water Authority rectify the gaps in the penetration tests, and connect all the water suppliers (that by the Water Authority should be connected) to the Cybernetic Center.



Summary

In recent years, there has been an exacerbation of cyber threats to the computer systems of the water and sewage system in Israel. It is recommended that the Authority Council and the Water Authority regulate the water suppliers' obligation to operate a monitoring and control system and a cyber incident protection system, to prepare information security plans, and to anchor in water security rules the Water Authority's power to instruct the water suppliers in the cyber field. The Authority is also recommended to connect all the water suppliers to the Cybernetic Center. It is further recommended that the Water Authority complete the cyber audits of corporations and other water suppliers that have not been audited in the past two years and increase the corporations' preparedness for cyber-attacks.



Report of the State Comptroller of Israel | Cyber and
Information Systems | 2022

Ministry of Education

**Special Audit Report
– Cyber Protection of
Information Systems
in the Ministry of
Education and of
Matriculation Exams
and Grades**



Special Audit Report – Cyber Protection of Information Systems in the Ministry of Education and of Matriculation Exams and Grades

Background

Most of the information the Ministry of Education collects, keeps, and manages regarding matriculation exams and grades is sensitive information about students and employees, including over 100,000 records. As such, its security must be at the highest level according to the Protection of Privacy Regulations (Data Security), 2017 (Protection of Privacy – Data Security Regulations). The Ministry's duty is to safeguard the information and ensure that it is used only for the purposes for which it was provided or for fulfilling its obligations according to the law. Hence, the Ministry should ensure that the information and data will not be altered or deleted, and will be disclosed only to authorized parties under their role, or to those the information concerns, such as the students or their parents, institutions of higher education and other parties for whom the matriculation certificate and student grades are required.

Another aspect requiring measures to prevent damage to databases is cyber-attacks, the frequency of which is increasing and causing significant and wide-ranging damage. The motives are varied, including the intention to harm the systems themselves and disrupt the regular and ongoing operations of the organization, society, and even the state, for extortion, altering information to garner benefits and reap profits, and as a technological challenge in and of itself.



Key figures

about
1.39 million

matriculation exam notebooks evaluated by the Ministry of Education in the 2021 school year (September 2020 – October 2021)

about
125,000

12th-grade students took the matriculation exams in 1,299 schools in the 2021 school year

about
12,000

exam notebooks suspected of being irregular in the 2021 school year

832

versions of questionnaires formed by the Ministry of Education for 62 subjects in the 2021 school year

about
2,200

cyber incidents handled by the National Cyber Directorate in 2021

33%

the increased rate of cyber incidents handled by the National Cyber Directorate in 2021 compared to the previous year

about NIS
467.6 million

the Examination Department budget in 2021

about **5%**
instead
of **8%**

the rate of the cyber protection budget allocated by the Ministry of Education from the information technology budget in 2020 (5%) compared to Government Resolution 2443 stipulating 8%

Audit actions

From February 2021 to May 2022, the State Comptroller's Office examined information security in the Ministry of Education and the information security of the central information systems supporting the management and operation of matriculation exam grades and the IT (Information technology) environments in which they operate. The examination was conducted at the Ministry's headquarters, in the Examinations Division, and in the Digital Information Technology Administration, at the Center for Grading Matriculation and Final Exams (the 'Marbad'), which an external company operates. A completion examination was conducted at the Government's Cyber protection Unit (YAHAV) and the Israel Police.

This report was submitted to the Prime Minister on December 6, 2022.



Under the authority vested upon the State Comptroller in Section 17(c) of the State Comptroller's Law, 1958 [Consolidated Version], considering the government's reasoning, consulting with the bodies entrusted with the security of defense information, in coordination with the Knesset chairman, and as the subcommittee did not convene, it was decided to publish this report while classifying as confidential parts thereof. These sections will not be submitted before the Knesset or published.

Key findings

-  **Conducting a risk assessment and penetration tests and implementing the annual work plan** – as of October 2021, over three years after the Ministry of Education conducted a comprehensive risk assessment of its selected core systems and a penetration test regarding System A, the ministry did not conduct a comprehensive risk assessment and penetration tests of its core systems as frequently as required by the Protection of Privacy – Data Security Regulations – once every 18 months. Of the seven tasks defined as "critical" or "high" risk level in the Ministry's 2019 work plan and determined to be carried out in 2019, as of October 2021, the Ministry has completed three tasks and has partially addressed the remaining four tasks.
-  **The Ministry of Education's preparedness for disaster recovery** – the Ministry of Education did not perform specific drills for restoring information and for disaster recovery as required by the Government's Cyber protection Unit (YAHAV) guideline "Backing up and restoring information." It also did not perform a drill to restore one of its computer systems completely.
-  **The Ministry of Education's compliance with the obligations promulgated under the Protection of Privacy – Data Security Regulations** – it was raised that three years after the entry into force of the Protection of Privacy – Data Security Regulations (in May 2018), the Ministry compiled the database structure documents, the definitions of the database, and the inventory list for only five (10%) of the 50 databases registered in the Registry of Databases. In the "Students" database definition document, the identity of the information security officer was not updated, and the inventory list is incomplete.
-  **The appointment of a Cyber Protection Officer, convening of a Cyber Steering Committee, and budget allocation for cyber protection** – from the end of 2020 until October 2021, the Ministry of Education did not staff the position of Cyber Protection Officer. The Cyber Steering Committee did not convene at the frequency required – at least once every six months. The Ministry also did not comply with the guideline, by which at least 8% of the information technology budget must be allocated for cyber



protection. In practice, the rate of the dedicated budget allocated for this purpose in 2019 was about 5.66%, and in 2020, it decreased to about 5.06%. It should be noted that the Ministry of Education stated in its response that in June 2022, a Cyber Protection Officer was appointed and that in 2022 (after the audit completion), it convened the Steering Committees for Information and Cyber Security twice.

Information Security on Network A – network A serves all users who are not employees of the Ministry of Education, including schools, teaching staff, students, parents, and suppliers. It is also accessible to Ministry employees according to their needs. Company A provides the Ministry with the network's central infrastructure services. Following are the key findings regarding Network A:

- It was raised that, a specific component and the network and information security equipment, which is under the care of Company A according to the engagement contract, are not directly accessible to the Ministry. The Ministry also does not request the company to periodically report the definitions and rules established for the rest of the network equipment and information security under its control, although, it is required to ensure that the definitions and regulations of the rest of the network equipment and information security meet the requirements in the engagement contract, the Ministry of Education's needs, and the Government's Cyber protection Unit guidelines that apply to it.
- The Ministry of Education did not ask for references documenting how Company A handled its calls, nor did it require it to send a file of the action records (the log file), allowing it to monitor the records documenting the actions performed in the systems.
- System E, which is supposed to allow monitoring of changes in the rules of specific protection components and controlling them, was not implemented on components under the control of Company A.
- The Ministry did not connect Network A to the government SOC¹.

Information Security on Network C – the process of the inspection and evaluation of the exam notebooks used by the examinees to answer the exam questionnaires is managed in Network C. Regarding Network C, the audit raised as follows:

- The network is protected by an outdated version of a specific protection system, which is unsupported by its manufacturer since September 2019. As of November 2021, a specific updated protection system has not yet been fully implemented in Network C.

1 The government command and control center for cyber threats – Security Operation Center (the Government SOC).



- Inconsistencies arose in this network regarding specific components for information security.
- In January 2020, the manufacturer stopped supporting the operating system of certain types of servers that are used, among others, Network C.
- Network C does not have a component that performs a specific control operation at the infrastructure level, as recommended in the guidelines.
- Server A and Server B of Network C are not separated; this allows certain employees access to Server B, even though they should not have such access. A copy of a specific database (DB) is kept on Server A, and it is accessible to authorized users who have been given access to this server. It was raised that those users also have access to a specific database even though they are not authorized to have such access.

 **Information Security on System D** – the files of the scanned exam notebooks and the computerized exam notebooks are loaded onto System D. Access to the system is granted, through the internet, to about 4,000 external evaluators who examine the exam notebooks and enter scores for them. Concerning this system, the audit raised the following:

- The evaluators connect to the system using personal computers that are not managed or hardened by the Ministry of Education and their connection is partially secured.
- The actions performed in System D are registered and documented in the log files, but they are not audited or monitored.
- Six out of eight users whose job was defined in System D under a specific definition received privileges that go beyond their role, not according to the "need to know" principle²; sometimes, there is no unique identification of users or details of the actions performed.
- Files are transferred between System D and the Ministry of Education (or its other suppliers) without being checked whether they contain any risk of harm, even though the regulations require a specific action when transferring information on the public network or the internet. Some files contain sensitive information that is transferred from System D to the Ministry through interfaces that are not sufficiently secure, increasing the risk of sensitive information leakage and damage.
- As part of a particular examination carried out by the State Comptroller's Office on System D, it was raised that the installation of the user side (Client) and the server

2 The "need-to-know principle" – minimizes to the extent possible the parties authorized to be exposed to the particularly sensitive information assets and provides transparency within the Ministry regarding information assets with lower security clearance classification.



side (Server) and the checking of the permissions are not as required by the Government's Cyber protection Unit guidelines.

 **Information security on System B** – system B is used to register the students taking the matriculation exams; About 250 of the schools also use it to enter the students' annual grades (the pre-matriculation grades). Regarding this system, the following was raised:

- 64% of users have not logged into the system for nearly five years – between March 2017 and January 2022; 19% of the users logged into the system about three to five years ago at the latest (in 2017–2019), and only 12% of the users logged into the system in the last year – January 2021 to January 2022. This raises concerns about granting access to the system to parties who do not need them.
- As of September 2021, the Ministry of Education did not scan files in a whitening (anti malware) system before transferring them to Environment B. As of November 2021, the external company did not scan the same files before importing them into Environment A or uploading them in System D.

 **System G on Network B** – the Ministry of Education did not regulate a procedure for the process of updating matriculation grades in System G, the entities involved, those responsible for each step, and the control over the process. Gaps arose in the Ministry of Education's monitoring and control mechanisms. The Ministry also does not perform retrospective audit – it has not regulated a process for receiving a regular periodic report of the actions performed in the system and locating activities suspected of being abnormal. The system also does not allow internal audit in a specific aspect.

 **Unauthorized distribution of matriculation exams** – the audit found seven groups in instant messaging applications operating in the Jewish sector and the Arab sector, where the unauthorized distribution of questionnaires and the solutions to the questionnaires took place. In 2018–2020, the Ministry of Education filed only four complaints at the Israel Police for the offense of "obtaining by fraud" following the unauthorized distribution of matriculation exam questionnaires or answers. It should be noted that in 2020 the Ministry disqualified more than 16,000 exam notebooks due to suspicion of violating the purity of the exams.



Changing the model of the distribution of exams – in 2015, the Ministry established a ministerial team to examine the preparation for the matriculation exams. In 2018, it mapped and analyzed the processes and risks in the Examination Division through an external company. As a result, the Ministry changed the matriculation exam distribution model. Among other things, it purchased and installed hundreds of iron safes in the schools, in which it keeps the matriculation exam questionnaires, allowing it to control its opening time remotely.

Key recommendations

-  It is recommended that the Ministry of Education convene the Cyber Steering Committee twice a year; implement the annual work plan on time; perform risk assessments and penetration tests once every 18 months; allocate at least 8% of the information technology budget to promote cyber protection under Government Resolution 2443 and the Government's Cyber protection Unit's (YAHAV) guidelines.
-  It is recommended that the Ministry of Education require references documenting Company A's handling of its calls and receive monitoring and audit reports, reports of the rules of a specific protection component, and definitions of the equipment for which Company A is responsible. It is further recommended that the Ministry of Education consider implementing measures to monitor the security of the components under the control of Company A, and connect Network A to the government SOC.
-  It is recommended that the Ministry of Education complete the implementation of the updated version of a specific protection component in Network C and upgrade the operating systems of Network C's servers that the manufacturer no longer supports. It is recommended that the Ministry of Education require the companies that operate the Center for Grading Matriculation and Final Exams ('Marbad') on its behalf to integrate the missing information security systems. It is also recommended that the Ministry establish capabilities for specific documentation and control of Network A and set alerts to detect risks of harm to the network.
-  It is recommended that the Ministry of Education perform periodic backup recovery drills and disaster recovery drills; to separate Server A and Server B of System D in certain aspects; and that a specific database is not used on Server A.
-  It is recommended that the Ministry re-examine the evaluators' connection model to System D from personal computers using a partially secure connection; that the Ministry ensure that the companies operating the Center for Grading Matriculation and Final Exams ('Marbad') on its behalf will follow the "need to know" principle and enable access



to information according to the user required information for performing their work only; and that the Ministry improve the monitoring and control capabilities in System D.



It is recommended that the Ministry of Education implement the white system in Network A and Network C. Regarding the transfer of sensitive information between its systems and external systems, the Ministry of Education should improve its protection capabilities against risks potentially causing harm or disruption to its systems and the information therein, under the Protection of Privacy – Data Security Regulations.



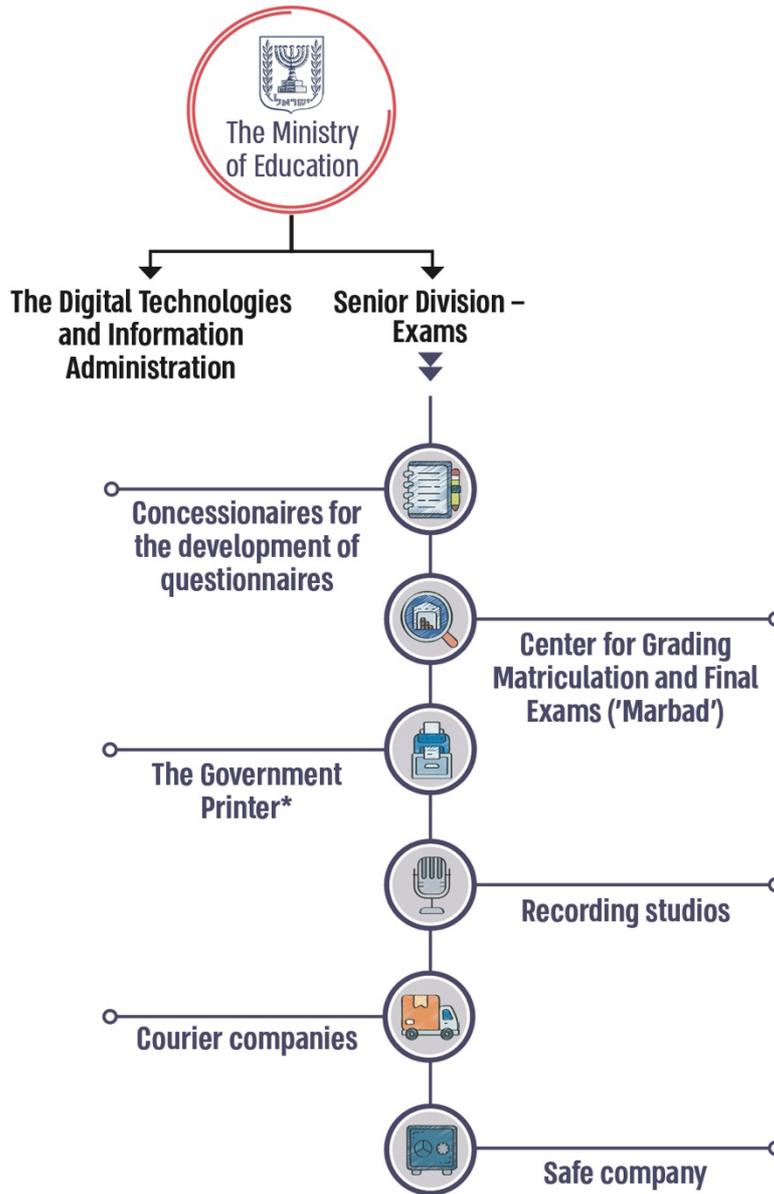
It is recommended that the Ministry of Education examine the list of those authorized to access System B and the permissions granted to them and perform a permission check among System B users, emphasizing changes made to the approvals. It is also recommended to consider implementing an automatic mechanism canceling access to the system of a user who has not logged into it for a period to be defined.



It is recommended that the Ministry of Education and the Israel Police consider tools to contend with the unauthorized distribution of the matriculation exams and the distribution of answers to them before they are over, for example, through monitoring and proactive checks on the various platforms where questionnaires and answers are distributed, including social networks and instant messaging applications.



The key entities involved in the management and operation process of matriculation exams



In purple – external entities

According to information collected during the audit, and processed by the State Comptroller's Office.

* The Government Printer is an auxiliary unit in the Ministry of Finance. Its primary role – the execution and production of printing work for the government ministries and auxiliary units through self-production or engagements with external subcontractors.



Summary

The Ministry of Education collects, saves, and manages considerable information about the matriculation exams. This is sensitive information, and its security should be at the highest level. The audit raised several deficiencies in information security – both in the maintaining proper information security governance in the Ministry of Education and in external outsourcing parties, and in the technical areas of implementing information security and cyber protection tools, systems and mechanisms under the Protection of Privacy – Data Security Regulations and the Government's Cyber protection Unit (YAHAV) guidelines.

The findings in the report and the basic problems may endanger the integrity, availability, confidentiality, and reliability of the matriculation exam scores. There is also the concern of harm to the principles of exam purity. The State Comptroller's Office recommends that the Ministry of Education rectify the deficiencies raised in the report, including complying with the schedules established in work plans in information security and cyber protection, improving and increasing the level of information security and cyber protection in all its systems and infrastructures. It is also recommended that the new system managing the matriculation grades, which the Ministry says it is developing, will contend with the findings raised in this report regarding the security of the information of the matriculation exams and matriculation grades.