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

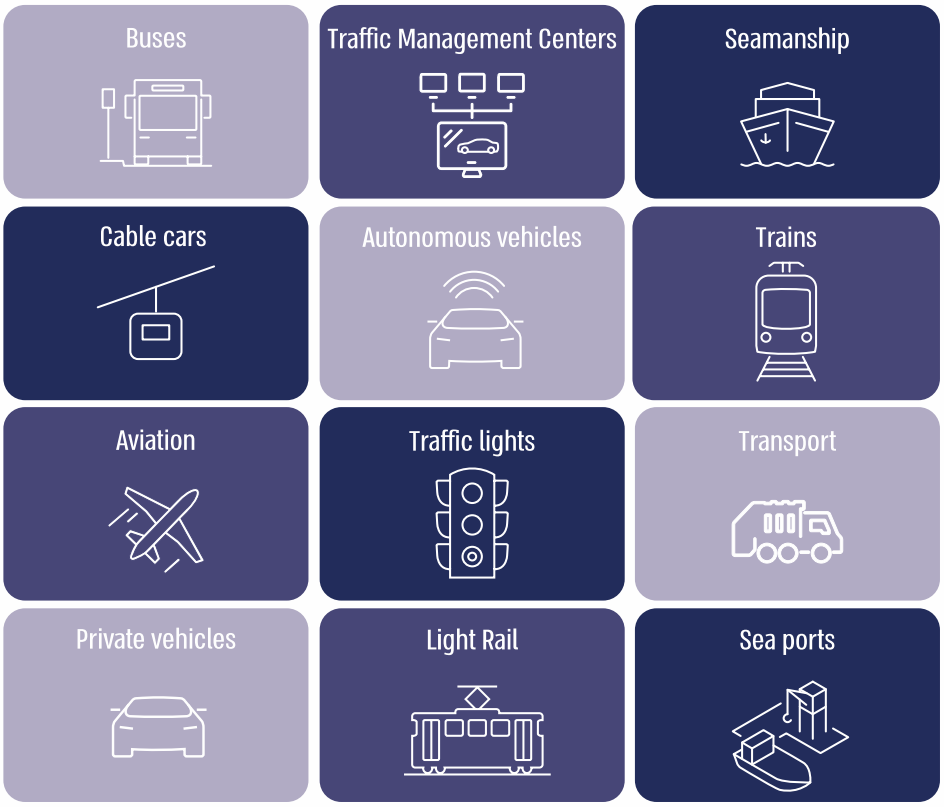
The Ministry of Transport and Road Safety is setting the policy in the Transport sector and the services of the Transport systems at sea, air, and land. The Transport sector includes entities of various types – governmental, public, and private, operating in various fields: maritime transport, land transport,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

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

7 years

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 mesures. 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 equirements, 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.

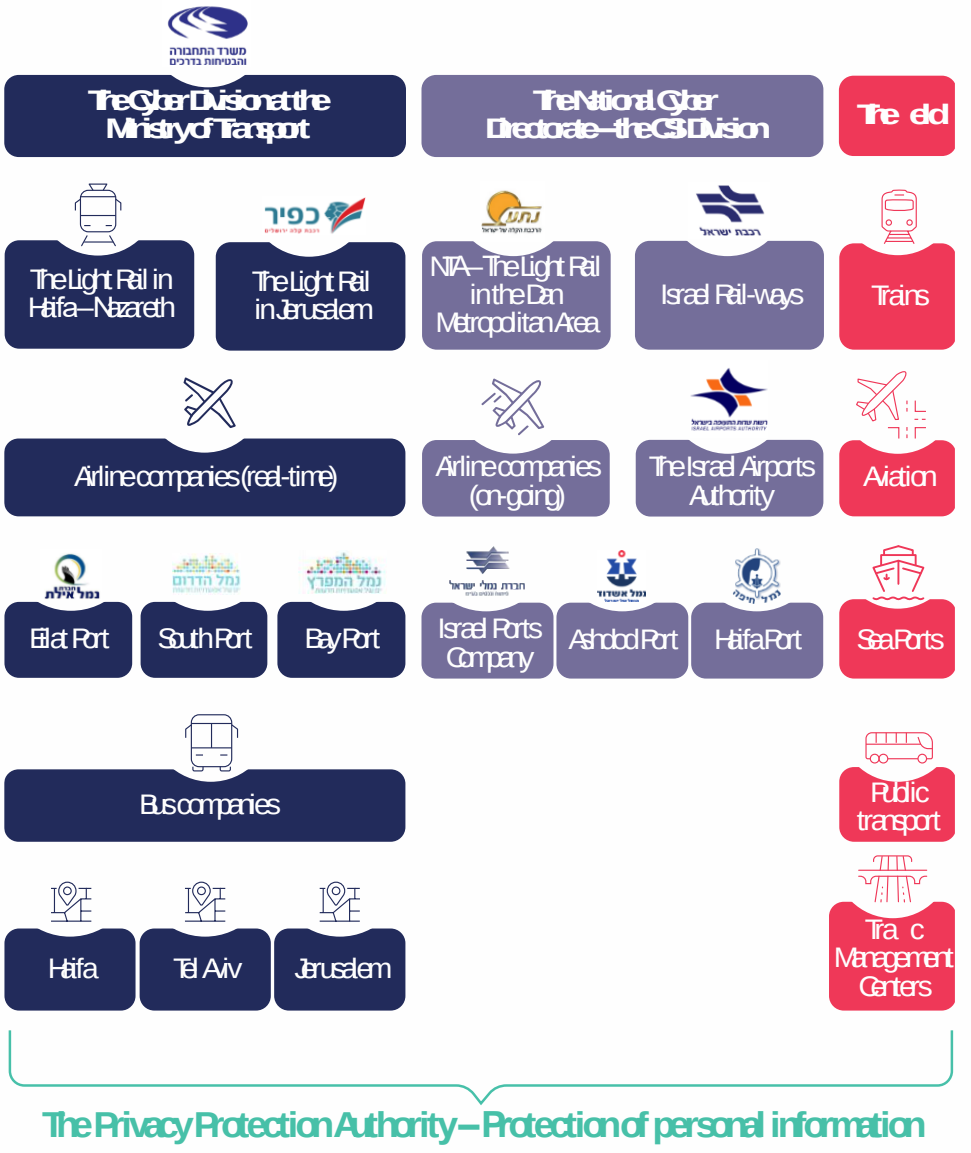
- Given the questionnaire and the penetration test findings regarding cyber security in transport systems, it is recommended that the Ministries of Interior and Transport, in cooperation with the National Cyber Directorate, regulate their responsibilities and establish appropriate procedures. Thus, cyber 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.

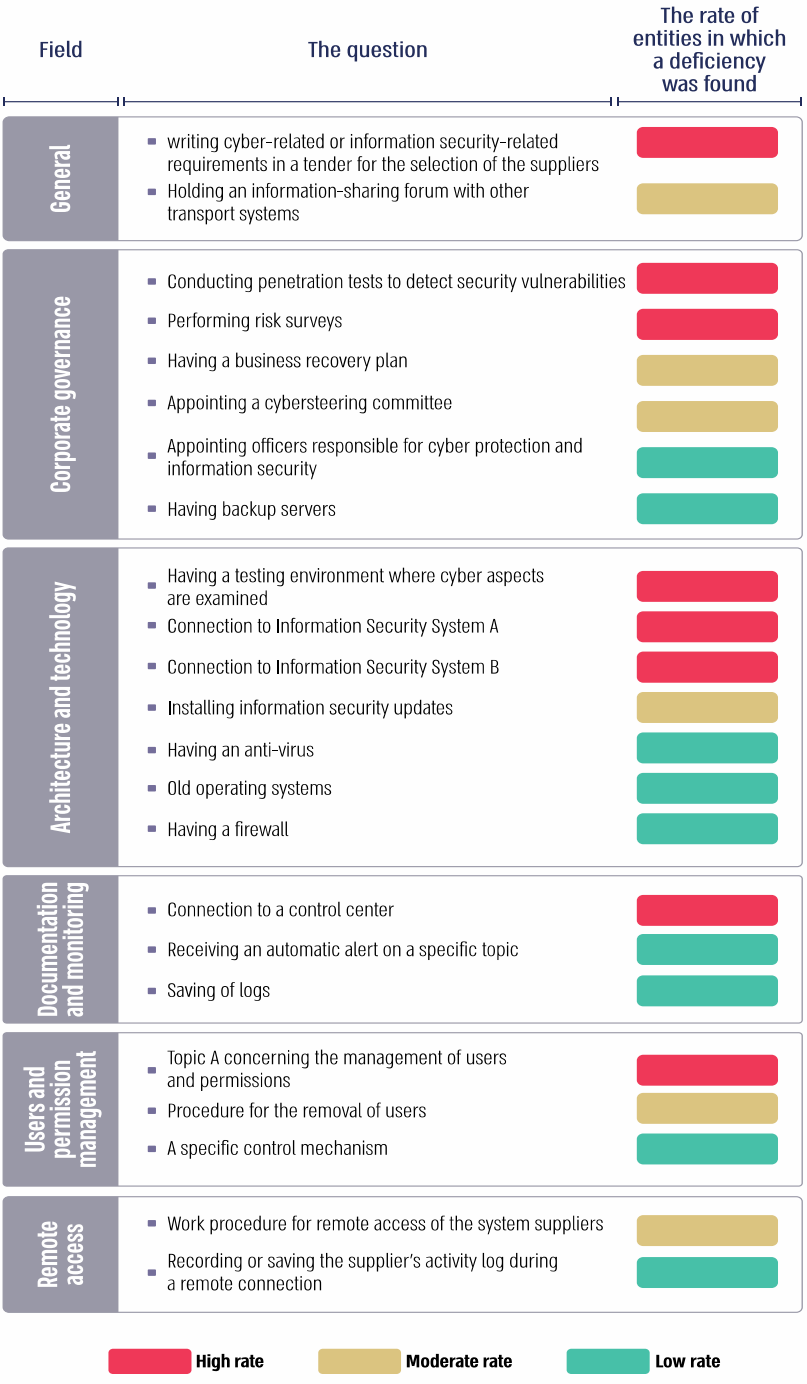
- Given the questionnaire findings, the entities examined should evaluate the situation and determine a work plan to rectify the deficiencies. It is recommended that all the authorities where systems in the field of transport are installed conduct risk surveys and penetration tests on their systems and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



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.