



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.