State of Israel

Report of the State Comptroller

Cyber and Information Systems

May 2026

Jerusalem

Foreword

The State Comptroller's annual audit report on Cyber and Information Systems is hereby submitted to the Knesset in accordance with the provisions of the State Comptroller Law, 5718-1958 [Consolidated Version]. This report addresses key aspects of cyber protection, information security, and digital services within the public sector.

In recent years, the digital domain has emerged as a fundamental infrastructure underpinning the activities of the State of Israel. Information systems, online services, and digital work processes currently constitute the operational foundation for government ministries, emergency bodies, public authorities, and citizen service systems. While digital transformation offers numerous advantages – including the streamlining of public services, enhancement of accessibility, resource optimization, and reinforcement of functional continuity – it concomitantly engenders elevated risks associated with cyber threats, information breaches, and vulnerabilities in information system protection. This prevailing reality necessitates that all public entities ensure their systems are secure, reliable, accessible, and resilient in both routine times and during emergencies.

Cyber protection and information system security presently constitute the cornerstones of good governance in the contemporary state. Digital systems aggregate personal, financial, and security-related information on a massive scale and serve as essential infrastructure for government ministries, emergency bodies, and critical public services. In an era marked by escalating cyber threats, and particularly during emergencies and crises, the state must undertake advanced preparations to guarantee system integrity, safeguard citizens' privacy, and maintain uninterrupted, secure, and reliable public service delivery. Strengthening this domain is not only a technological requisite, but also a fundamental pillar of national security, public confidence in state institutions, and governmental capacity to deliver efficient, advanced, and accessible public services to all citizens.

The importance of enhancing the protection of information systems and digital infrastructures is especially pronounced given the complex security environment that the State of Israel has faced in recent years. During this period, hostile entities have increasingly attempted cyberattacks, while state bodies have been required to assure operational continuity and the provision of essential public services even under emergency conditions. These developments have demonstrated that information systems, digital services, and remote work infrastructures function not merely as administrative and technological instruments, but as integral components of national resilience and the state's ability to operate continuously, efficiently, and securely.

The four chapters of this report address distinct yet complementary dimensions within the domain of cyber and information systems in the public sector:

- **Information Systems and Information and Cyber Security at the Ministry of Foreign Affairs**
- **Cybersecurity in Remote Work during Routine Times and Emergencies**
- **Information System Security at the Ministry of Construction and Housing**
- **Online Public Services: The National Identification System and the Government Personal Area**

The first three chapters underwent a confidentiality process in the Knesset State Audit Committee sub-committee, which decided not to bring them in their entirety before the Knesset, but to publish only parts thereof, to protect the state's security.

The audit findings reveal deficiencies in preparedness, risk management, supervision, and the execution of government policy in this field, alongside only partial progress in enhancing digital service accessibility and in deploying advanced protection and control mechanisms. Although each report examines a specific subject area, their collective results demonstrate that strengthening the protection of information systems, ensuring operational continuity, and advancing the digital transformation of public service constitute national challenges necessitating systemic, coordinated, and sustained intervention.

The audit of **Information Systems and Information and Cyber Security at the Ministry of Foreign Affairs** was conducted during the Swords of Iron War and identified deficiencies in the management and development of the Ministry's information systems, as well as in the domains of information security and cyber protection. Given its role, the Ministry of Foreign Affairs represents a key target for cyber-attacks perpetrated by a range of adversaries, from hackers to state actors. The audit findings underscore the necessity of enhancing the supervisory and control mechanisms governing the Ministry of Foreign Affairs' management of information systems and information security, in order to ensure the proper functioning of its IT infrastructure and to augment the protective measures for the Ministry and its assets.

One chapter of the report addresses **the implementation of government policy for promoting digital public services through the national identification system and the government personal area**. The audit disclosed that despite numerous governmental resolutions since 2014 concerning the enhancement of online services, and notwithstanding the

registration of approximately 4.6 million citizens within the national identification system, policy implementation remains partial and sluggish. Only 16% of mapped services are connected to the identification system; only approximately 23% of the identified online forms are managed through it; and merely 233 out of thousands of government services have been made accessible via the personal area. Furthermore, it was found that only 15 of 258 local authorities have connected to the national identification system, and the integration of government ministries and other public bodies with these systems is limited, thereby hindering the public's ability to receive comprehensive, straightforward, and accessible digital government services.

Another chapter addresses **the security of information systems within the Ministry of Construction and Housing**, which maintains millions of records containing personal and sensitive data about citizens, housing beneficiaries, and contractors. The Ministry utilizes numerous information systems, and in 2025, its information and cyber security budget amounted to approximately NIS 6.5 million, representing roughly 9% of its total computing budget. The audit identified significant shortcomings in the management of information and cyber security within the Ministry, including deficiencies in access authorization controls, inadequate application of risk management processes, absence of sufficient alert mechanisms, and incomplete registration of databases as mandated by law. These findings gain particular significance in light of the substantial increase (approximately 130%) in cyber alerts received by the Ministry in 2024, underscoring the critical importance of effective protection of the state's information assets.

The report further examines **cyber protection in remote work**, which has become integral to the operations of public and security bodies in recent years, particularly during the COVID-19 pandemic and the Swords of Iron War. The audit assessed the readiness of critical agencies, including the Israel Police and the National Fire and Rescue Authority, to manage the cyber threats associated with remote work. Findings exposed certain gaps in the adaptation of protection and control mechanisms with respect to extant risks. Moreover, a penetration test conducted by the Office of the State Comptroller on the Fire and Rescue Authority's remote work system revealed deficiencies. These outcomes highlight the necessity to finalize work plans and to enhance cyber protection preparedness within the nation's critical bodies.

Overall, the report findings indicate that Israel's advancement toward a sophisticated digital government mandates sustained investment in cyber infrastructure, risk management, oversight, and enforcement,

coupled with close collaboration among all public entities. Ensuring adequate protection of information systems and digital services is not merely a technological requirement, but a necessary prerequisite for maintaining public trust, safeguarding citizens' privacy, and securing the proper and continuous functioning of public services.

The audited entities are responsible for acting expeditiously and effectively to rectify the deficiencies identified in this report.

I extend my gratitude to the personnel within the Office of the State Comptroller who prepared this report with professionalism, thoroughness, dedication, and a strong sense of mission. It is my hope that the report's findings and recommendations will contribute to the strengthening of cyber and information security systems within the public sector and enhance the quality of services delivered to the citizens of Israel.

We express our hopes and prayers for the swift recovery of the injured, the rehabilitation of the hostages who have returned to us and to their families, the safe return of all evacuees to their homes, the safety of our soldiers, and the success of the security forces in safeguarding our nation.

Matanyahu Englman
State Comptroller
and Ombudsman

Jerusalem,
May 2026