Report of the State Comptroller of Israel | July 2024

Prime Minister's Office

Protection of Computerized Information Within the Prime Minister's Office

Protection of Computerized Information Within the Prime Minister's Office

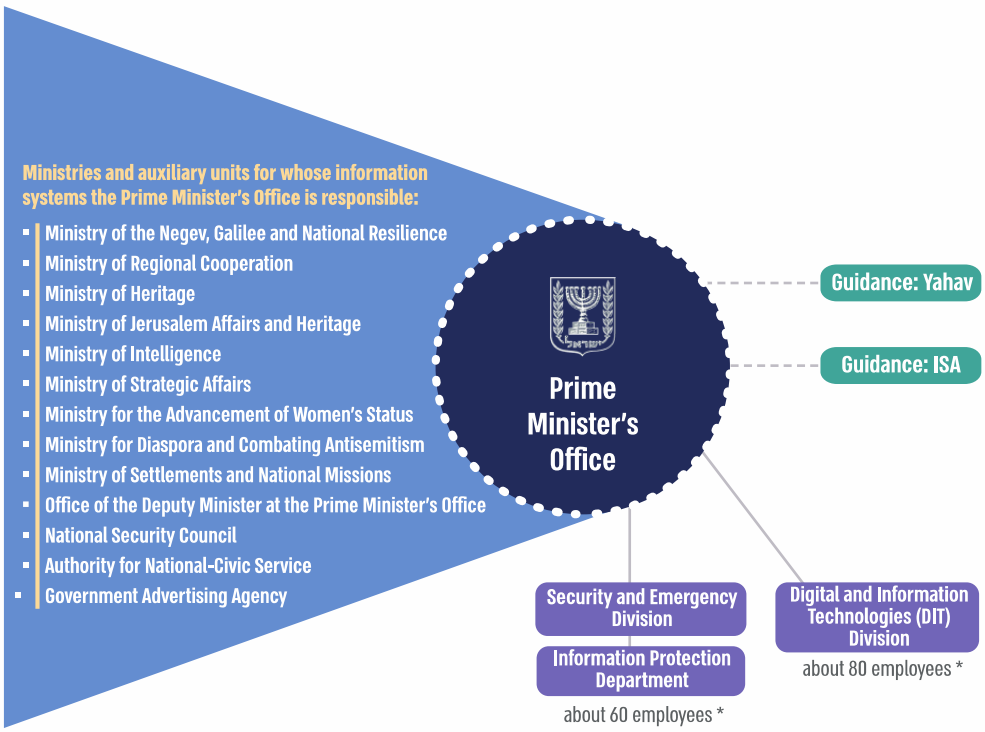
Background

The Prime Minister's Office is responsible for the implementation of the political, economic, social, and administrative vision of the Prime Minister and the government regarding key agenda issues. The Office provides information systems management services and data protection to 13 auxiliary units and to other government ministries. The National Security Council (NSC) operates as an auxiliary unit of the Prime Minister's Office, serving as the headquarters for the Prime Minister and the government in regard to Israel's foreign and security affairs. All bodies and units receiving information systems management and data protection services from the Prime Minister's Office shall be referred to hereinafter as the Prime Minister's Office.

The computerized systems within the Prime Minister's Office contain substantial information, including sensitive information, information that is considered 'classified' from a security perspective, and information categorized as highly confidential. Any damage in regard to this information, including its leaking, disruption, or unavailability, could result in severe long-term harm to the security of the State of Israel or its critical infrastructure, particularly during times of war when incidents of cyber-attacks increase. Therefore, the protection of classified information managed by the Prime Minister's Office is of utmost importance.

In terms of information protection, the Prime Minister's Office adheres to guidelines set forth by regulatory authorities, following the established protection doctrine set by the relevant regulator for each network. The professionals assigned to data protection within the Prime Minister's Office include the Senior Digital and Information Technologies Division (DIT Division), responsible for information technologies and the safeguarding of unclassified information, as well as the Information Protection Department within the Security and Emergency Division, which oversees the protection of classified information.

The General Organizational Structure of Digital Technologies and Information Protection in the Prime Minister's Office, the Ministries and the Auxiliary Units for Whose Information Systems the Prime Minister's Office is Responsible and the Bodies Guiding the Office



Source: The Prime Minister's Office, the DIT Division, Presentation 2022; The DIT Division, Cyber Defense Steering Committee Presentation, May 2, 2023; Regulation of Security in Public Bodies Law, 1998; Government Resolution 2443 (February 15, 2015).

* Employees in the Prime Minister's Office as well as employees hired by the Office (outsourcing). According to data from the Security and Emergency Division in the Prime Minister's Office, about 10 of the 60 employees in the Information Protection Department were involved in cyber defense.

Key Figures

low protection level

Prime Minister's Office's classified networks have a lower level of protection than required

about 49 million

attempted attacks on the remote connection service at the Prime Minister's Office in January-May 2023 alone

dozens

active users on a classified network at the Prime Minister's Office entered the network, contrary to the logical settings established by the Prime Minister's Office

Audit Actions

From March to August 2023, the State Comptroller's Office audited the protection of computerized information, primarily within the classified computer networks of the Prime Minister's Office. The audit included several key areas: the overall management of information protection within the Prime Minister's Office, including budgetary aspects; the user identification system and authorization management; the monitoring of systems within a specific network; the currency of operating system and software versions; and security of classified information. The audit focused mainly upon the Prime Minister's Office and the National Security Council (NSC), with supplemental examinations conducted at the Cyber Defense Unit ('Yahav'), the Israel Security Agency (ISA), and the Civil Service Commission.

For protection of state security, the sub-committee of the Knesset State Audit Committee decided not to bring this report before the Knesset in its entirety, but to publish only parts thereof, under Section 17 of the State Comptroller's Law, 1958. The confidentiality of this data does not prevent the understanding of the nature of the audit.

Key Findings

Overarching Management of Information Protection

- **Management of Steering Committees and Frequency of Meetings –** the Steering Committee for Cyber Protection is mandated to raise the level of cyber protection within the government ministry and to supervise the implementation of

such measures. The audit found several deficiencies concerning the operation of the steering committees in the Prime Minister's Office: the Committee for Information Protection did not convene with the required frequency from 2018 to 2022; the position of chairperson was unoccupied in 2020; between 2020 and 2022, the Committee was not chaired by the Director General of the Prime Minister's Office, contrary to government resolutions. The Committees for Protection of Unclassified Information and for Classified Information did not adequately address the process for examination and approval of annual work plans from 2019 to 2022.

- **Formulation of a Cyber Protection Policy and Risk Surveys –** the Prime Minister's Office approved the unclassified information protection policy in November 2018, but it has not been updated or validated for four and a half years, as required by the regulatory authorities' guidelines, despite significant organizational changes, including: the establishment of the Information Protection Department in the Security and Emergency Division, and the assumption by the Prime Minister's Office of responsibility for managing information systems and information security across other government ministries. The established information protection policy did not encompass all required areas, nor was it approved by the Director General as mandated. Furthermore, the risk survey conducted by the Prime Minister's Office did not adhere to the stipulated guidelines.

- **Control Over Cyber Protection Implementation in the Office –** the Steering Committee failed to address the findings calculated by way of the index created by "Yahav" (which assesses governmental administrative control regarding cyber protection), despite indicators reflecting a decline in the overall score of the Prime Minister's Office (from 86% to 68%) and a significant decrease in three levels of control: management responsibility and compliance and two other levels of protection.

- **The IT Budget of the Prime Minister's Office –** the execution of the Prime Minister's Office budget for information technologies under the regulation entitled "computing expenses" from 2018 to 2023 varied between about NIS 49 million and NIS 68 million annually. Data from the SIGMA (System for Integrated Government Management and Administration) System do not clarify the Prime Minister's Office's total IT budget or the specific allocation for cyber defense, impeding transparency regarding compliance with the government resolution to allocate 8% of the budget for cyber defense. Moreover, the classification of the Office's expenses across 11 different budget regulations complicates data aggregation, hindering the Steering Committee's ability to confirm adequate resource allocation for cyber protection. From 2018 to 2023, the Steering Committee for Unclassified Information did not ensure sufficient resources were allocated for cyber protection, as required by the government resolution.

- **Discharging of Core Positions by the Digital and Information Technologies Division Director –** from 2021 and continuing until mid-2023, the Director of the DIT Division discharged, in effect, three out of five key positions in the information technology sphere of the Prime Minister's Office. Additionally, in 2018, 2019, and 2022, the Director served as the interim chair of the Steering Committee for Protection of Unclassified Information. The dual responsibilities may impair the performance of the tasks for which he is responsible. Furthermore, managing the DIT Division while performing the duties of an information security officer, may hinder the ability to supervise and regulate information security tasks effectively. The Civil Service Commission permitted the Prime Minister's Office to forgo one position – the Office's technology manager – without providing reasons.

User Identification and Authorization Management

- **Identification for Accessing the Network –** access protocols to the networks of the Prime Minister's Office do not adhere to the standards outlined by regulatory authorities. Additionally, the logical settings established for user passwords are inconsistent with established guidelines.

- **Management of Network Access Privileges –** the Prime Minister's Office exhibits deficiencies in managing access privileges across its computer networks. Deficiencies were identified in the identification system that was set up and implemented by the Prime Minister's Office, including with respect to regular network access password updates, which fail to align with established office procedures. Such deficiencies have arisen regarding user accounts in various groups. These deficiencies compromise system protection and pose significant risks to the integrity, confidentiality, and availability of information on the Office's networks, and this requires prompt rectification.

- **Management of Permission Groups on a Specific Network –** in addition to network access permission, employees are also given permissions set for the work groups to which they belong. In a particular network that was examined, permission groups were found that were no longer relevant, such as a group that was assigned to the team of a former minister without portfolio who left office more than a decade ago, as well as dozens of "duplicate" groups with the same name, each of which included different members. The Prime Minister's Office lacks centralized supervision regarding the contents and subject matter of each authorization group.

- **Setting Expiration Dates for Accounts –** the setting of expiration dates for user accounts is vital for effective management and oversight of permissions and enables control over permissions granted. The Prime Minister's Office has implemented expiration dates for only a portion of active user accounts (ranging from 19% to 62% across networks examined). Moreover, certain accounts designated as expired remain "enabled", with findings indicating 6% to 40% of accounts retaining "enabled" status post-expiration in the networks examined. Additionally, several

accounts were identified with expiration dates set far into the future, between 2033 and 2071, rendering them ineffective.

- **Control of User Management –** in a specific network reviewed within the Prime Minister's Office, there has been a lack of supervision concerning user group permissions and employee access approval, as required by regulatory guidelines, for a period extending from early 2020 to August 2023.

- **Access to Networks of Inactive Accounts –** the Prime Minister's Office permits access to networks through inactive user accounts, with findings raising that between 18% and 43% of accounts remained enabled despite non-usage. Furthermore, access is granted via accounts belonging to former employees. Permitting access to networks through these accounts allows unauthorized parties – internal or external – to view and use information, and therefore poses a significant risk to the information stored on networks.

- **Suspicion of Unauthorized Account Use After End of Employment –** audit findings raise suspicion that former employees accessed their accounts after they were no longer employed, or that others, in the Office or outside it, may have made use of these accounts, while being exposed to information on the Prime Minister's Office networks that they were not authorized to access and being able to perform actions that they were not supposed to perform. Among other things, the account of a former Minister and the account of a senior official in the Prime Minister's Office, who had long since finished their terms, were used. These suspicions require an exhaustive in-depth examination of each of the cases, to verify or dismiss any such suspicion.

Monitoring Systems in a Specific Network

- Monitoring operations on the network enables the detection of unauthorized attempts to access systems, identification of attacks, and support for recovery from information security incidents. It was found that the Prime Minister's Office did not activate the monitoring system in a specific network examined as required: certain network components were not connected to the Office's Monitoring System (SIEM), while others failed to generate LOG files. Additionally, the audit raised concerns regarding insufficiently established rules for monitoring systems, particularly in defining the scenarios that would trigger alerts. Consequently, the Office's capacity to detect system attacks and recover efficiently has been impaired.

- The Office also did not establish a standard duration for addressing alerts within the specific network examined. Furthermore, there were concerns regarding information security due to the partial staffing of the SOC position responsible for the same network, particularly in relation to high-severity alerts.

Currency of Versions of Operating Systems and Software

- **Systems Functioning After the End of Their Life Cycle**
  - In a specific network examined within the Prime Minister's Office, servers and several communication components were found to be beyond their support phase, thereby exposing them to discovered vulnerabilities. The utilization of these components by the Prime Minister's Office contravenes regulatory guidelines, and no adequate security measures have been implemented for their use, which would constitute a violation of the Privacy Protection (Information Security) Regulations, 2017.
  - Within the networks examined, there are servers and communication components operating with outdated versions of their operating systems, with the life cycle end date having long passed (between 17% and 27% of the servers on the networks examined). This situation leaves these servers susceptible to vulnerabilities associated with their operating systems, contravening regulatory guidelines.
- **Installation of Security Updates –** the Prime Minister's Office has not ensured timely installation of required updates for server operating systems, resulting in exposure of the Office's information systems to numerous vulnerabilities, including those frequently exploited by cyber attackers globally. A significant number of servers have at least six-month delays in critical security updates as of the examination date (July 2023).

Protection of Information in Classified Security Networks

- **Information Protection Level in Classified Networks Within the Prime Minister's Office –** the information protection level on the networks is lower than the required standards and does not meet regulatory requirements. This is particularly concerning as the Prime Minister's Office is a target facing constant threats at a critical severity level. The existence of classified networks with insufficient protection could lead to substantial damage to the State of Israel in various aspects, including political, security, economic, and reputational harm.
- **Information Protection on a Specific Classified Network Examined –** for more than a year and a half, from the date the Information Protection Department submitted its findings regarding information security on the classified network examined until the audit end date, no significant deficiencies identified during the examination were rectified. Consequently, this network remains at risk due to these deficiencies.
- **Resilience Testing and Protective Measure Installation on a Specific Classified Network –** the Prime Minister's Office has not conducted a penetration

test on this classified network, as mandated, for at least six years (from 2018 to 2023).

- **Prevention of Information Leakage –** the Prime Minister's Office has not implemented protective measures on the particular classified network equivalent to those installed on another classified network.

The State Comptroller's Office commends the Prime Minister's Office's response to the audit findings. The Prime Minister's Office stated that the recommendations of the State Comptroller Office were consolidated by the Digital and Information Technologies Division, responsibilities for implementation were assigned, and a timetable was established for the completion of implementation according to their designated urgency. The Office indicated that the relevant parties are committed to the matter and are dedicated to its advancement.

Key Recommendations

- The Prime Minister's Office should achieve the required level of protection for its networks in accordance with the guidelines set forth by regulatory bodies.
- The Prime Minister's Office should establish steering committees for cyber protection, led by the Office's Director General, and convene these committees as frequently as needed. These committees should review the information security work plans annually, make decisions on their approval, and document these decisions in meeting summaries. Furthermore, it is recommended that an updated policy for the protection of unclassified information be presented to the steering committee for review and approval, as required.
- The Prime Minister's Office should compile data on all available budgets for information technology management across all bodies it is responsible for, while also maintaining a separate budget record specifically for cyber defense initiatives. It is recommended that the Office formulate its information technology management budget requirements annually to minimize the need for significant budget increases throughout the year.
- The Prime Minister's Office should implement a mechanism to ensure appropriate protection when accessing the Office networks, adjusting logical access requirements accordingly. It is essential that passwords for all accounts active within the Office networks are changed at the required frequency.
- The Prime Minister's Office should: regularly update user groups established on the specific network examined and remove unnecessary groups; to assign expiration dates for all

temporary employee accounts; to develop a policy concerning expiration dates for tenured employee accounts; to ensure that individuals with expired account access are prohibited from network entry; and to establish an effective control system for managing access privileges across the networks.

- The Prime Minister's Office should revoke access privileges of employees upon their departure from the office, deactivate unused accounts, and ensure these accounts maintain an "inactive" status. It is also recommended that the Prime Minister's Office generate an "anomalies report" to identify irregularities in the management of access systems to the Office's networks.

- In collaboration with the Israel Security Agency, the Prime Minister's Office should conduct thorough inspections to investigate potential misuse of employee accounts post-employment, perform lateral inspections of all office networks, and act based on the inspection findings.

- The Prime Minister's Office is required to finalize activities pertaining to the monitoring system on the specific network examined: connect all system components to the SIEM, ensure each component generates LOG files, and establish rules for analyzing the resultant data. Additionally, it is recommended that the Prime Minister's Office set a standard duration for handling alerts from the monitoring system.

- The Prime Minister's Office should ensure that products are not utilized beyond their life cycle and guarantee that security updates are installed in accordance with the manufacturer's instructions.

- The Prime Minister's Office should address deficiencies related to the security of information on the specific classified network examined, verify the protection measures in place, and conduct penetration tests as necessary, acting based on the results.

- The Prime Minister's Office should mitigate the risk of information leakage from its defense targets.

- Regulatory bodies responsible for supervising the Prime Minister's Office concerning information security on the Office networks should ensure that the Prime Minister's Office rectify any deficiencies found in the audit.

Summary

The Prime Minister's Office is responsible for the planning and implementation of the policy of the government and Prime Minister regarding key agenda issues. The Prime Minister's Office has information systems which are used by sensitive organizations, including the Prime Minister's Bureau, the Government Secretariat, the Prime Minister's Military Secretariat, and the National Information System. Additionally, operating therein is an auxiliary unit serving as the headquarters for the Prime Minister and the government in regard to Israel's foreign and security affairs. The audit raised several overarching deficiencies concerning information protection within the Prime Minister's Office, including with respect to the work of cyber protection steering committees operating within the Office and the management of the Office's information technology budgets.

The computerized systems within the Prime Minister's Office contain substantial information, including sensitive information and information that is highly classified. The required protection for classified information is at the highest level. The audit found that the network protection level within the Prime Minister's Office is inadequate, which poses a risk of significant detrimental effects for the State of Israel in the political, security, economic, and reputational spheres.

Deficiencies were found in managing access privileges to the computerized systems of the Prime Minister's Office. A monitoring system was not activated on one network as required, diminishing the Office's ability to detect and respond to system attacks adequately. Furthermore, essential updates for various systems, including server operating systems, were not implemented, leaving information systems vulnerable to cyber threats widely exploited by attackers worldwide.

The State Comptroller's Office commends the Prime Minister's Office's response to the audit findings. The Prime Minister's Office stated that the recommendations of the State Comptroller's Office were consolidated by the Senior Digital and Information Technologies Division, responsibilities for implementation were assigned, and a timetable was established for the completion of implementation according to their designated urgency. The Office indicated that the relevant parties are committed to the matter and are dedicated to its advancement. The Security and Emergency Division stated it would initiate operations in 2024 to supervise and control unclassified information networks concerning functional continuity and information leakage.

The responsibility for addressing the deficiencies found in the audit regarding the management of information technologies and security of computerized information within the Prime Minister's Office lies with the Director General of the Prime Minister's Office, who also chairs the Cyber Defense Steering Committee. It is imperative for the Prime Minister's Office to rectify the deficiencies outlined in this report.

The Israel Security Agency and the "Yahav" Unit within the National Digital Agency, tasked with advising the Prime Minister's Office on information security, should ensure the audit findings rectifications.