Report of the State Comptroller of Israel – Cyber and Information Systems | November 2024

The National Insurance Institute

Information Security and Cyber Protection at the National Insurance Institute

Information Security and Cyber Protection at the National Insurance Institute

Background

The National Insurance Institute (NII) maintains an extensive database containing information from numerous organizations and government bodies, amounting to many terabytes (TB) in size. This database grows at about 10% annually, and it encompasses information on all residents of the State of Israel from birth until death. NII's databases are mandated to uphold a high level of security under the Privacy Protection (Information Security) Regulations, 2017[1].

In July 2023, a Supreme Steering Committee for the Protection of Computer Systems in Israel[2] decided that the NII meets the required criteria and should be guided as a Critical Cyber Infrastructure body (CCI). Consequently, the Committee recommended the inclusion of the NII in the Fifth Schedule to the Regulation of Security in Public Bodies Law, 1998, to be guided by the National Cyber Directorate (NCD) under this law. As of April 2024, the audit completion date, approval has not yet been received for adding the NII in the Fifth Schedule of the law above. In alignment with its transformation into a CCI body, the NII has initiated proactive measures to enhance its protective measures, following the designated methodology for CCI bodies.

As of February 2024, the NII is subjected to tens of thousands of cyberattack attempts daily. A cyber incident affecting the NII could significantly harm the privacy of millions of citizens and residents receiving services from the NII, potentially disrupting operations and impairing the ability to disburse benefits (old age, disability, subsistence, unemployment, reserve benefits). A pertinent example of a severe information security incident at the NII, as defined in the Regulations, occurred in February 2022 when an identity theft event was reported, exposing the personal information of 2,000 citizens to unauthorized access.

1 Regulation 1, the Second Schedule and Fifth Schedule to the Information Security Regulations.

2 Government Resolution B/84 of 2002, which determined that a supreme steering committee should be established for the protection of computer systems in the State of Israel, whose role would be to examine which bodies would be defined as "essential" and therefore in need of cyber protection. Responsibility for this protection was assigned to the Israel Security Agency (ISA). In 2016, as part of an amendment to the Regulation of Security in Public Bodies Law, 1998, this responsibility was transferred from ISA to the National Cyber Directorate.

Key Figures

10 years

the NII's cyber protection policy has not been updated, though significant changes have occurred since then. 50% of the procedures that, according to the Protection of Privacy Regulations (Data Security), are required to be included in every organization's information security procedure do not exist at the NII

tens of thousands

the number of alerts on cyber-attacks on the NII per day that require investigation by a single analyst working at the NII Security Operations Center (SOC)

over 2 years

the time during which the Cyber Steering Committee headed by the CEO did not convene – from the beginning of 2022 to January 2024

0

penetration tests were conducted on the central system of the NII

87%

of the Information Security Regulations are only partially implemented in the NII. No periodic audits are conducted to ensure compliance with regulations

numerous bodies

receive information from the NII through information-sharing systems in which information security gaps were discovered

Audit Actions

From July 2023 to April 2024, the State Comptroller's Office audited information security and cyber protection at the National Insurance Institute (NII), focusing on compliance with the Information Security Regulations. The audit addressed several key areas, including cyber protection policies and procedures, risk management, information transfer from the NII to external entities, logical and physical protection, business continuity, response to cyber incidents, and supply chain management. The audit was performed at the NII, the Prime Minister's Office – the National Cyber Directorate, and the Ministry of Justice – the Privacy Protection Authority.

The Knesset State Audit Committee sub-committee decided not to submit data from this chapter before the Knesset to protect the state's security under Section 17(a) of the State Comptroller's Law, 1958 [Consolidated Version].

Key Findings

- **Information Security and Cyber Protection Policy –** the NII has not updated its information security and cyber protection policy for nearly a decade, since 2014, despite significant changes in the risk landscape. This is inconsistent with its policy, requiring annual discussions and approvals of the information security policy. At the time of the audit, the policy document had been updated to draft status and approved in March 2024 by the Acting CEO of the NII; However, discussions have not yet been held by the Information Security Steering Committee as required by the policy document. Additionally, the policy document lacks explicit references to critical issues outlined by recognized standards, such as asset management, classification, and compliance controls with the Information Security Regulations.

- **Information Security Procedures –** the NII information security procedures inadequately address 6 of the 12 issues (50%) mandated by the Information Security Regulations that should be included within the information security procedural framework. Regarding 4 of the 12 issues (33%), existing procedures had not been updated in a decade, and in respect of 2 issues (17%), the most recent update dates are unspecified.

- **The Cyber Protection Steering Committee –** the Cyber Protection Steering Committee, led by the CEO, did not convene from early 2022 until January 2024, contrary to NII policy requiring biannual meetings. This lack of meetings resulted in the absence of a governing body to approve the cyber protection policy, endorse annual work plans,

monitor implementation, or present the cyber protection status, including gaps, significant events, and threats, to the organization's leadership. Furthermore, during the first committee meeting in January 2024, the cyber protection status was not presented to the NII's Acting CEO, the draft policy was not approved, and other essential topics defined in the committee's appointment letter were not discussed.

- **Risk Management –** the NII does not maintain a comprehensive inventory of all assets and business processes, nor does it classify them based on their level of importance to the organization, as mandated by the Information Security Regulations and industry standards, including the norms included in the protection doctrine[3]. The NII has identified a limited number of essential systems, mapping about one-third of those deemed most critical for examination in the survey. An ineffective risk management process lacking comprehensive asset mapping raises concerns that the risk management will not optimally reflect the main risks to which the organization is exposed, indicating that resources and actions to mitigate risks may not align adequately with the actual risk levels associated with the organization's assets. Additionally, the NII does not conduct risk surveys for its databases every 18 months, as required for organizations managing databases subject to high-security standards.

- **Penetration Tests –** the NII does not perform penetration tests on its databases under the Information Security Regulations and its internal policy document. As a result, about 7% of tests conducted relate to systems linked to the central system of all NII databases. Additionally, the NII does not monitor rectifying identified vulnerabilities, leading to persistent high-severity deficiencies that remain unresolved and expose the NII to potential risks. Penetration tests are also not executed on the central system, and there is a noted deficiency in knowledge and resources concerning implementing such tests within the NII and the NCD.

- **Logical Protection –** deficiencies were found across multiple domains in the NII logical protection.

- **Identifying and Handling Cyber Incidents –** deficiencies were found in the NII's capability to identify and manage cyber incidents. The NII does not have dedicated crisis management teams, including an incident response team (IR) and a digital forensic and incident response team (DFIR). A management team for cyber incident supervision was established at the end of January 2024 but has not yet convened, received training, or participated in drills. Additionally, gaps were found in the operations of the SOC, where the staffing team has not undergone specialized training. The SOC is supervised by the Infrastructure Division instead of the Information Security Division, creating a disparity between the need to analyze tens of thousands of alerts daily and allocating only one

3 The National Cyber Directorate, Implementation Guide for the Organization's Cyber Defense Version 2.0 (June 2021).

analyst to the SOC. This situation raises concerns regarding the timely identification of genuine threats or at all.

- **Business Continuity –** deficiencies were found in the NII's business continuity capabilities across several critical areas. The current draft business recovery procedure lacks essential elements typical of a comprehensive business continuity plan, including up-to-date mappings of vital processes and associated risks, clearly defined recovery objectives, and allocating necessary resources. Moreover, the draft procedure contains recovery priorities established in 1991 and ratified in 2013, which are outdated. Furtheremore, the NII has not conducted a disaster recovery drill in the past three years, and gaps were found in restoring data from backups.

- **Supply Chain Risk Management –** the NII does not have a formal supply chain procedure or a comprehensive mapping of its ICT suppliers and their risk classifications. Additionally, the tenders it issued do not include an information security appendix that mandates supplier compliance with controls aligned with the supply chain methodology requirements. Moreover, the NII does not audit its ICT suppliers, which presents a risk to the organization due to potential vulnerabilities in critical suppliers. In the few instances where audits have been conducted, deficiencies were identified.

- **Transfer of Information from the NII to External Bodies –** the NII shares information with numerous external bodies via information-sharing systems with security gaps. Furthermore, the NII does not ensure that the information shared with public bodies aligns with the approval given by the Information Transfer Committee. There is also a lack of periodic audits regarding the expiration of information transfer interfaces, which leads to continued information sharing beyond the five-year limit specified in its procedures.

- **Compliance with Legal and Regulatory Requirements –** the NII does not have a work plan for a continuous monitoring of its databases adhering to the Protection of Privacy Regulations, as mandated by Regulation 3 to said Regulations. Given that the NII database, classified as an extensive database, contains sensitive information of many terabytes, it is mandatory to implement such an organized plan to achieve an adequate level of security. Furthermore, 87% of the Protection of Privacy Regulations (13 out of 15) are only partially complied with by the NII.

Internal Penetration Testing Team – the NII employs a dedicated team of trained resilience testers who routinely conduct infrastructural and applicable penetration tests for various systems and applications. Still, no tests are performed on the central system.

Supply Chain – in the new tenders, the NII has incorporated requirements for supplier audits and their obligation to report incidents in the information security chapter.

The Iron Swords War – during the Iron Swords War, the NII undertook urgent measures to assist victims of hostilities, families of the hostages, families of evacuees, and reserve personnel. These measures included developing new services for these populations, creating interfaces for information transfer to other entities, and implementing solutions enabling NII's employees to work remotely to ensure uninterrupted service.

Backup Site (DR) – the State Comptroller's Office commends the NII for relocating the backup site (DR) to a new location in March 2024, during the audit.

Key Recommendations

- The NII should revise its information security and cyber protection policy document to address issues that require attention according to established standards and present the updated document to the Information Security Steering Committee. Furthermore, it should periodically update the document to align with evolving risks, as mandated by the NII Security and Cyber Protection Policy.
- Given concerns that critical issues in the NII's information security are not addressed according to changes in the organizational environment and emerging cyber threats and risks, the NII should update its information security procedures to encompass the obligations set forth by the Information Security Regulations. Additionally, existing procedures that have not been revised in the last two years require updating.
- Following the replacement of the acting CEO at the NII after the first Cyber Steering Committee meeting, and considering that significant issues such as the level of cyber protection were not discussed during the committee's session, the NII should reconvene the Cyber Steering Committee promptly. This meeting should focus on presenting the cyber protection levels and other key issues outlined in the committee's appointment letter and obtaining approval for the draft policy.
- The NII should catalog all its assets and business processes, classify them according to their importance to the organization and adhere to the requirements of the Information Security Regulations.
- With guidance from the National Cyber Directorate, it is recommended that the NII systematically conduct information security risk surveys following accepted methodologies, such as the protection doctrine, and ensure that the risk surveys consider risks posed to Critical Cyber Infrastructure bodies on the national level. The results and a plan to address identified deficiencies should be submitted to the National Cyber Directorate, which functions as the professional supervisor of the NII.

- The NII should engage content experts to conduct penetration tests on the central system. Given that some CCI bodies have comparable systems, the National Cyber Directorate should establish a forum to facilitate knowledge sharing among relevant parties, which will also evaluate a national systemic response for testing these systems.
- The establishment of dedicated crisis management teams, including an incident response team (IR) and a digital forensic and incident response team (DFIR), is recommended for the NII. Additionally, the NII should convene and train the management team to handle cyber incidents effectively.
- In collaboration with the National Cyber Directorate, the NII should enhance the capabilities of its Security Operations Center (SOC) to detect and respond to cyber incidents while also addressing operational gaps within the SOC. It is further recommended that the SOC be subordinate to the Information Security Division.
- With assistance and guidance from the National Cyber Directorate, the NII should perform a comprehensive mapping of its suppliers under the recommendations of the National Cyber Directorate. It is also recommended that a template for an information security appendix be developed for tenders, outlining the supplier's contractual obligations and compliance requirements under the National Cyber Directorate's supply chain methodology.
- Risk assessments and information security audits should be conducted for active information-sharing systems. When information security vulnerabilities are identified, the NII should implement compensating controls.
- The NII should expedite an audit of compliance levels of significant databases it holds concerning the Information Security Regulations in line with regulatory requirements. This audit should be conducted regularly.

The National Insurance Institute's Level of Compliance with the Information Security Regulations

Topic	The audit findings
Database definitions document	Partially found
Information Security Officer	Partially found
Security Procedure	Partially found
Mapping of the database systems and performance of a risk survey	Partially found
Physical and surroundings security	Found
Information security with respect to management of manpower	Partially found
Logical protection – topic 1	Partially found
Logical protection – topic 2	Partially found
Logical protection – topic 3	Partially found
Documenting of security incidents	Partially found
Mobile devices	Partially found
Secured and updated management of database systems	Partially found
Communications security	Partially found
Outsourcing	Partially found
Periodic audits	Not found

Prepared by the Office of the State Comptroller.

Summary

The NII maintains an extensive database containing many terabytes (TB) of information regarding all residents of the State of Israel from birth to death. It is imperative to ensure a high level of security for this database, in compliance with the Privacy Protection Law and the Privacy Protection Regulations, due to its classification as a primary target for potential attacks, with tens of thousands of suspected incidents occurring daily. The potential damage to this database is critical, especially during the ongoing conflict known as the Iron Swords War, during which the NII has a crucial role in supporting the injured, evacuees, and reservists.

In June 2023, the NII was designated as a Critical Cyber Infrastructure body (CCI body) and commenced processes to enhance its cyber defense under a dedicated doctrine for CCI bodies and the guidance of the National Cyber Directorate. During the Iron Swords War, the NII implemented urgent measures to assist victims of hostilities, the families of the hostages, evacuees, and reservists. These measures included developing new services for these populations, creating interfaces for information transfer to other entities, and identifying solutions that allow staff to work remotely, thus ensuring uninterrupted service delivery.

This report's findings highlight significant deficiencies in information security management at the NII and its preparedness for cyber threats. Numerous gaps were found across all areas pertinent to information security, including deficiencies in the detection and management of cyber incidents, inadequate logical security measures, an outdated business continuity plan, and low recovery capacity in the event of a disaster. Collectively and individually, these findings risk the information's confidentiality, integrity, and availability within the NII databases.

Additional findings indicate only partial compliance with the Information Security Regulations and a lack of capacity within the organization's information security division to fulfill specific responsibilities.

The Acting CEO of the NII, the management team, the Cyber Steering Committee, and the National Cyber Directorate, as the professional guide, should identify the material cyber risks facing the organization and develop a comprehensive work plan to address the information security gaps highlighted in this report.