



Report of the State Comptroller of Israel | Cyber and
Information Systems | 2022

The Israel Defense Forces

Management of Biometric Information in the IDF and its Cyber Protection



Management of Biometric Information in the IDF and its Cyber Protection

Background

Biometric information is a unique physiological human characteristic that a computer can measure. The risks posed to a biometric database are significant since, unlike other means of authentication such as a certificate, password, or physical means – biometric data cannot be revoked or replaced due to theft or leakage of information.

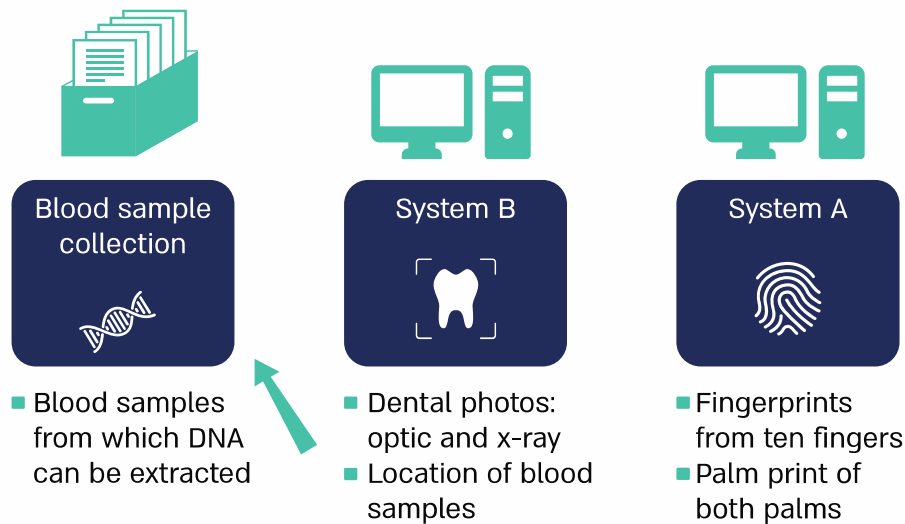
The biometric information the IDF collected from conscripts is used to identify fatalities and is stored in three identification databases (a fingerprints and palm prints database, a dental photographs database, and a blood samples collection). In the acquisition process, as part of the enlistment process, the following means of identification are taken from every soldier enlisting in the IDF: fingerprints and dental photographs. Furthermore, with the conscript's consent, blood samples are taken to produce a DNA sample when necessary. The identification process of fatalities is conducted by comparing the biometric data taken from the conscript to those taken from the fatality.

The IDF should act under its cyber security policy, the Protection of Privacy Law, 1981, and the Protection of Privacy (Data Security) Regulations, 2017 (Data Security Regulations). According to the Data Security Regulations, a database containing biometric information and over 100,000 records is required to meet a high level of security. The Regulations detail how the level of security settings for the database should be maintained.

The IDF has three critical information systems to manage the identification process: System A and System B, which manage the identification database, have been classified by the IDF and are required to meet a high level of security under the Data Security Regulations. System C manages the records of the fatality, including its identification process. The Weapons Officer at the Chief Personnel Officer Headquarters in the Personnel Directorate is the project manager of the identification systems and is responsible for formulating the systems' cyber security response. The 'Tachlit' branch in the 'Shahar' Unit is responsible for developing and maintaining the systems. The primary systems users are the 'Meitav' Unit (in the acquisition process) and the Identification and Burial Branch in the Military Rabbinate (in the fatality identification process).



Following is a diagram presenting the means of identification and the information stored therein:



Key figures

3 information systems

manage the means of identification

hundreds of thousands

of fingerprint records are kept in the IDF identification database

7 years

have passed since the IDF's cyber security policy was updated

26 years

in which the privacy protection General Staff directives were not updated. Thus, they do not refer to the 2017 Data Security Regulations

0

number of risk surveys and penetration tests conducted to examine the protection level of the identification systems since their establishment in 2005–2006 (about 16 years ago)

50%

2 of the 4 acquisition stations for collecting photographs of the oral cavity in the enlistment process are shut down from August 2021 (more than six months)

95%

of the dental photographs found in the identification database were of insufficient quality

1 of every 87

of those currently serving in mandatory service and standing army officers (1.15%) allowed only one capability mean, raising concerns about their identification in the future



Audit actions



From August 2021 to April 2022, the State Comptroller's Office audited the "Biometric Information Management in the IDF and its Cyber Protection". The audit was conducted in the IDF: in the Personnel Directorate – at the Strategy, Digital and Systems Branch (ADAM) and in the Headquarters of the Chief Personnel Officer; in the intake and sorting section – at the Meitav Unit; in the Shahar unit – at the Tachlit branch; in the Military Rabbinate – at the Identification and Burial Branch. Completion examinations were conducted at association A and the Privacy Protection Authority at the Ministry of Justice.

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



The cyber security policy – the IDF's cyber security policy includes part of the topics that the Government's Cyber protection Unit (YAHAV) defined as mandatory in the security policy such as protection of records, logical and physical protection, and the organizational structure, but does not include management and classification of assets, the supply chain, human resources and compliance with legal requirements (such as Data Security Regulations). Furthermore, the cyber security policy has not been updated since April 2015, for seven years, during which there have been technological changes and changes in the obligations applicable to the IDF on information security under the Protection of Privacy (Data Security) Regulations from 2017.



The cyber security response – System A and System B were classified with moderate security even though these systems are required to meet a high level of security under the Data Security Regulations, and despite the significant damage that may be caused by the leakage of sensitive biometric information stored in these systems. Moreover, the



IDF's identification systems do not have a detailed documented cyber-security protection response, including the specific protection requirements for these systems according to their classification.



Information security officer – the IDF has several entities dealing with various aspects of information security of information systems, including the Cyber Protection Unit at the Center of Computing and Information Systems (Mamram), the Information Security Department (Mahbam), the Weapons Officer and cyber-security policy officials in the Computer and IT Directorate. However, it has no single entity responsible for all the information security aspects of the identification systems which his role and areas of responsibility were defined under Regulation 3 of the Data Security Regulations and the IDF cyber security policy.



Compliance with Data Security Regulations – the Personnel Directorate has no regular monitoring plan to evaluate the degree of the identification databases' compliance with the Data Security Regulations requirements, and no audits were carried out on these issues. It was also found that the General Staff directives on privacy protection have not been updated since they were written in 1996 (26 years ago). Therefore, they do not refer to the Data Security Regulations published in 2017. Moreover, the Privacy Protection Authority did not conduct audits and organization-wide supervision on the IDF databases in general and the biometric databases for identifying fatalities in particular, to ensure that the databases comply with the Data Security Regulations even though the IDF maintains databases containing sensitive and personal information about many citizens.



Database definitions document – the IDF did not formulate a definition document for the identification databases as required by the Data Security Regulations, including essential information about the databases and their purpose, such as detailing the main risks of harm to information security and contending with them.








Superfluous information – the IDF did not examine whether superfluous information was kept in the identification databases once a year, as required by the Regulations. The identification databases contain superfluous information, like biometric information of soldiers who passed away (deceased) and for whom no identification process was carried out. Biometric information of deceased persons may be more easily used for impersonation and identity theft since no one will complain about the use thereof.



Physical protection – the IDF did not formulate a dedicated physical security procedure for the identification systems as required by Regulation 4 of the Data Security Regulations, even though they store biometric, personal, and sensitive information requiring a high level of security. Disparities were also found in the physical security of the systems in Unit A as follows: physical protection and control of the entrances and exits, protection of the work environment, and environmental protection.



-  **Logical protection** – disparities were found at the level of logical protection in the following topics: authentication; access rights; access control survey; control over the execution of unauthorized operations; encryption mechanisms; and regular control for application protection processes.
-  **Business continuity** – the IDF did not develop a business continuity plan for the identification process that covers all the identification means processes and all the units involved in them, and it did not define which parts of the process are critical during an emergency incident. Furthermore, it did not conduct an emergency operation drill of the entire array required to identify a fatality. In addition, the following disparities were found: the IDF did not ensure that the systems were regularly accessible from alternate sites determined in advance; in the MAMRAM unit, no periodic drills were carried out to do a backup checkup to ensure their integrity and compliance with the data recovery; the physical collection of blood samples is kept in a single location, and there is no redundancy for the information therein by storing them in a different location.
-  **Integrity of the means of identification** – the IDF's biometric database containing hundreds of thousands of records is incomplete. The database contains several tens of thousands of records of mandatory service soldiers and standing army officers, which as of the audit completion in April 2022, lack the following means of identification: 0.5% of the fingerprints, 6.6% of the X-ray photographs, 32.8% of the oral cavity photographs and 3.8% of the DNA samples. Also missing are hundreds of fingerprints of soldiers who enlisted in 2016 and 2017 and several thousand dental photographs of standing army officers who enlisted in 1994–2004. In addition, by the Medical Identification Section audits it carried out in 2018–2019 about 95% of the dental and oral cavity photographs are of insufficient quality. The poor acquisition quality of the dental photographs was still not addressed by the audit completion in April 2022.
-  **Methodology for project management** – the methodology for project management in the IDF (Personnel Directorate Standing Order (PDSO) 10/1) published by the Planning Division is not specific to manage information systems projects and therefore does not include a detailed reference to mandatory issues that are required in accepted methodologies for the management of information systems projects. In addition, the methodology does not include tools that will help the entities in its implementation: standards, guidelines, working procedures, and uniform templates in project management. Moreover, the methodology does not address project management according to the "agile"¹ method, even though the IDF develops systems according to this methodology, for example, the new B System.
-  **Project management** – in the identification systems, no fundamental documents such as detailed requirements documents or intermediate products as required in work processes according to accepted methodologies for managing information systems

1 (In Hebrew) The amalgamation of the words "nimble" and "flexible".



projects and according to PDSO 10/1. Without these essential documents and intermediate products, there is a risk that the developed systems do not suit the users' requirements.



Project manager – the identification systems were not managed according to accepted methodologies for project management; this includes gaps found in the following matters, under the purview of a project manager: preparation of work plans and the monitoring of their execution, client management and participation, bringing the projects up for discussion at steering committees meetings, risk management, change management, and bag management.



Identification of fatalities during a mixed mass fatality disaster (MFD) involving civilians and soldiers – the use of the Center for the Collection of Fatality Data ("Ha'Tzvi Center") of the Military Rabbinate during a mixed MFD involving civilians and soldiers was not regulated. Furthermore, although the IDF maintains a database containing hundreds of thousands of records of civilians and soldiers, including unique means of identification such as fingerprints and palm prints, the possibility of using the identification databases held by the IDF for identifying victims during an MFD has not been thoroughly examined.









Increasing the IDF's work interfaces with the Privacy Protection Authority – in 2021, the IDF, in cooperation with the Privacy Protection Authority, began formulating a comprehensive work plan that will address the following: appointment of a Privacy Protection Officer in the various units, internal IDF informational activities to strengthen its privacy protection, the inclusion of the privacy protection in the audit carried out by the Personnel Directorate and amending the General Staff directives.

Outsourcing – during the audit, the IDF ensured that Company B, which provides technical support to System A, had secure access to the identification systems and audited this access.








Completing insufficiencies in means of identification – between the recruitments from February to March 2022, the IDF began acquiring identification means from the fighters using a mobile station with acquisition stations borrowed from the enlistment process.



Key recommendations

-  It is recommended that the Biometric Applications Officer presents to the IDF the regulatory document he drew up in December 2015 with the IDF Information Security Department (Mahbam) and examine together the need to update it according to the work format established with similar special bodies.
-  It is recommended that the Cipher and Security Center in the protection Division update the cyber-security policy and include the issues specified in accepted cyber-security policy such as the Government's Cyber protection Unit (YAHAV) directive on policy. It should update it periodically according to the technological changes and risks in the field, and meet the relevant requirements of the law and Regulations.
-  It is recommended that the Information Security Department periodically re-examine and validate the classification of the identification systems considering the current risks posed to the information stored in these databases and the risks due to an information leak. The Chief Personnel Officer Headquarters in the Personnel Directorate should ensure that the principles of the cyber security-policy are anchored in a cyber-security response document and implemented in the identification systems in stages of development and maintenance. In addition, it is recommended that the Chief Personnel Officer Headquarters in the Personnel Directorate verify every year that the systems' cyber-security response adequately contends with the risks faced at that time and with the current threat scenarios.
-  It is recommended that the IDF appoint an Information Security Officer responsible for the identification systems under the Protection of Privacy Law and Data Security Regulations.
-  The Personnel Directorate should prepare an ongoing control plan for the databases' degree of compliance with the Data Security Regulations and verify its execution once every two years or as part of a risk survey. It is further recommended that the Personnel Directorate, in cooperation with the Computer and IT Directorate, update the General Staff directives on privacy protection.
-  It is recommended that concurrently with the ongoing legislative amendment process, the Privacy Protection Authority will regulate the ability to supervise and enforce the information databases in the IDF, including the identification databases. It is also recommended that the Personnel Directorate, in cooperation with the Privacy Protection Authority, implement the work plan formulated following the meeting in May 2021, including promoting training in the IDF on compliance with Data Security Regulations and formulate a plan for training officials to serve as internal supervisors within the IDF.



-  The IDF should write a physical security procedure under the Data Security Regulations. Furthermore, Unit A, in cooperation with the IDF's information security officials, should protect the compound that was examined in the audit.
-  It is recommended that the Information Security Officer, in cooperation with the IDF Information Security Department (Mahbam), reduce the gaps in logical protection.
-  It is recommended that the IDF formulate a business recovery plan for the identification process, examine the entirety of the processes, the risks, and the consequences of their realization, and define the level of response given to each risk. It is also recommended that the IDF periodically conduct emergency drills covering all processes of identification means and the units involved in these processes.
-  It is recommended that the Personnel Directorate reduce the disparities in the acquisition of the missing identification means, prioritize its completions according to the nature of the soldiers' service (combat service, risk levels, etc.), the type of identification means (fingerprints) and the number of times they were called for completion. In addition, operate a mobile station to acquire identification means, including dental photographs.
-  It is recommended that the Personnel Directorate, in collaboration with the Planning Division, update the relevant procedures for managing information systems projects (10/01 and 10/6) so they include a detailed reference to the mandatory issues required in accepted methodologies for managing information systems projects and adapt the methodology for project management using the "agile" method. It is further recommended to form implementation tools of the methodology and establish a supporting body for project management (such as a PMO) to contend with this need.
-  It is recommended that the Chief Personnel Officer Headquarters in the Personnel Directorate manage the identification systems according to accepted methodologies for managing information systems projects and to PDSO 10/1 and formulate the required work documents according to these methodologies. The Personnel Directorate should formulate an orderly plan defining the areas of responsibility of the Chief Personnel Officer Headquarters in the Personnel Directorate as the project manager of the identification systems in preparation for the next steps in the development of these systems and that it implements it according to accepted methodologies.
-  It is recommended that the National Emergency Management Authority (NEMA), in cooperation with the Authority for Evacuation, Relief, and Treatment of Victims in an Emergency, examine the existing response and the necessary response to identifying victims during a mass fatality disaster (MFD), regulate the division of responsibilities between the different bodies and promote the use of Ha'Tzvi Center as a national fatality concentration station during a mass fatality disaster. In this framework, it is recommended to examine the feasibility of using the IDF's database and other databases to identify fatalities during a mass fatality disaster. It is recommended that the matter be examined in cooperation with the representatives of the Privacy Protection Authority



and representatives of the IDF: the Personnel Directorate, the Military Rabbinate, and representatives of the Military Advocate General's Office.

The risks posed to the identification databases





The identification databases' compliance with the Data Security Regulations requirements

Regulation	Topic	The audit findings
2	Database definitions document	Non-existent
3	Information security officer	Not appointed
4	Security procedure	Non-existent
5	Mapping of the database systems and the performance of a risk survey	Partially found
6	Physical and environmental security	Partially found
7	Information security in personnel management	Partially found
8	Access authorization management	Partially found
9	Identification and verification	Partially found
10	Access control and documentation	Partially found
11	Documentation of security incidents	Partially found
12	Mobile devices	Found
13	Secure an updated management of the database systems	Partially found
14	Communications security	Found
15	Outsourcing	Found
16	Periodic audits	Non-existent



Summary

The IDF manages identification information systems identifying fatalities. These are systems managing biometric databases including medical, personal, and sensitive information. Therefore, it is required that the security level of the databases be high under Data Security Regulations.

The findings of this report present significant information security gaps found in these sensitive systems, and indicate non-compliance with some Data Security Regulations and non-implementation of requirements included in the cyber-security policy documents. This state of affairs creates a risk of damage to the reliability, integrity, availability, and confidentiality of the information in the databases.

The report includes additional findings on the operation and management procedures of the identification information systems. Among other things, it was found that the information systems are not managed efficiently and according to an orderly methodology for managing information systems projects, resulting in the concern that the identification systems will not be able to fulfill their purpose. It was also found that the project manager needed to prepare work plans for the identification systems and ensure that the establishment and management of the systems met the accepted goals of content, schedules, costs, and customer satisfaction.

The head of the Personnel Directorate should rectify the deficiencies and examine the recommendations in this report.

