September 9 2022

Information Security Act: Parliament approves draft

Walder Wyss Ltd | Tech, Data, Telecoms & Media - Switzerland

JÜRG SCHNEIDER

HUGH REEVES

FLORIAN ROTH

- Introduction
- Ordinances subject to public consultation
- Consultation deadline
- Notification obligation of operators of critical infrastructures

Introduction

On 18 December 2020, Parliament approved a draft Information Security Act (ISA) with the aim of bolstering proper information security practices within all levels of the federal government. The ISA is expected to enter into force mid-2023.

Rather than setting out detailed obligations and standards itself (which could be quickly outdated), the new ISA is designed as an overarching law establishing a harmonised framework within which the competent federal authorities in the relevant sectors can implement adequate information security measures through ordinances and directives. This framework law provides in particular for risk management procedures, uniform information classification categories, security checks on people, and federal support for operators of critical infrastructures in the field of information security (for further details see "Parliament adopts Information Security Act").

The ISA leaves room for the Federal Council to enact more detailed regulations, including concretising the new law's scope of application.

Ordinances subject to public consultation

On 24 August 2022, the Federal Council opened public consultation on three new ordinances and a revision of an existing ordinance implementing the ISA:[(1)]

- the Information Security Ordinance (ISO);
- the People Security Checks Ordinance (PSPO);
- the Business Security Procedure Ordinance (BSPO); and
- the Revised Ordinance on Federal Identity Management Systems and Directory Services (FIMDSO).

The draft ISO combines, supplements and replaces two previous ordinances, the Cyber Risks Ordinance[(2)] and the Information Protection Ordinance.[(3)] Article 2 of the draft ISO clarifies that the ISA will apply to:

- the Federal Council;
- central government agencies and the Swiss army; and
- decentralised government agencies to the extent that:
  - they use or access certain information technology (IT) resources subject to high security clearance standards; or
  - they process classified information of the federal government (paragraphs 1 and 2).

It further clarifies that organisations outside the federal government entrusted with administrative tasks are exempt from the ISA to the extent that they do not qualify as critical infrastructures (paragraph 5). The ISO will contain a list of decentralised agencies that are subject to the ISA. Finally, the ISA will partially apply to public or private organisations operating critical infrastructures.[(4)]

The PSPO will regulate personal security audits used to assess whether persons performing a sensitive activity might pose a risk to the confederation's information security. According to the new law, these audits are to be reduced to the minimum required to identify significant risks to the confederation. The PSPO will replace several existing ordinances and directives in the field.

The BSPO will set out detailed rules on the business security procedure applicable to the confederation's procurement proceedings with respect to security-sensitive services or goods.

With its revision, the scope of FIMDSO is extended to decentralised government agencies that have access to the centralised government's IT resources.

Consultation deadline

The public consultation will be open until 24 November 2022. Anyone interested is welcome to submit their view on the draft ordinances.

Notification obligation of operators of critical infrastructures

With respect to operators of critical infrastructures (OCIs), it should be noted that the Federal Council opened a public consultation on a revision of the ISA (even before its full entry into force). In addition to the support offered by the federal government to OCIs, this revision will provide for a general obligation of OCIs to report cyberattacks with considerable damage potential to the National Cyber Security Centre (NCSC) (for further details see "Federal Council in favour of requiring critical infrastructures to report cyberattacks"). The consultation proceedings were closed on 23 May 2022 and are pending evaluation. The draft bill provides guidance on who will be qualified as an OCI for the purposes of the notification obligation.

Pursuant to article 74d(1) of the draft ISA, a cyberattack must be notified to the NCSC if there are reasons to believe that the attack:

- jeopardises the functioning of the respective critical infrastructure or another critical infrastructure;
- was initiated or implemented by a foreign state;
- led or could lead to a leak or manipulation of information; or
- remained undetected for more than 30 days.

A cyberattack must always be reported if it is accompanied by extortion, threat or duress against an OCI or its personnel (paragraph 2).

For further information on this topic please contact Jürg Schneider, Hugh Reeves or Florian Roth at Walder Wyss by telephone (+41 58 658 58 58) or email (juerg.schneider@walderwyss.com, hugh.reeves@walderwyss.com or florian.roth@walderwyss.com). The Walder Wyss website can be accessed at www.walderwyss.com.

Endnotes

(1) The press release and documentation on the public consultation can be accessed here: German, French, Italian; and here: German, French, Italian. (last visited on 29 August 2022).

(2) SR 120.73.

(3) SR 510.411.

(4) As per article 2 paragraph 5 of the ISA, article 75-81 will apply to operators of critical infrastructures. These provisions, however, do not set out obligations of such operators but rather a framework for support to them by the federal authorities in connection with information security risks.