Implementation plan for Finland's Cyber Security Strategy 2024-2035

This implementation plan should be read in parallel with the Cyber Security Strategy.

Contents

1. Introduction

Finland's Cyber Security Strategy 2024-2035 was adopted by Government Resolution on 10 October 2024. Its implementation plan sets out the measures that are necessary for achieving the objectives, together with the associated responsibilities and metrics. The implementation plan will be approved by the steering group of state secretaries overseeing the government security management operating model development project (VSI OHRY).

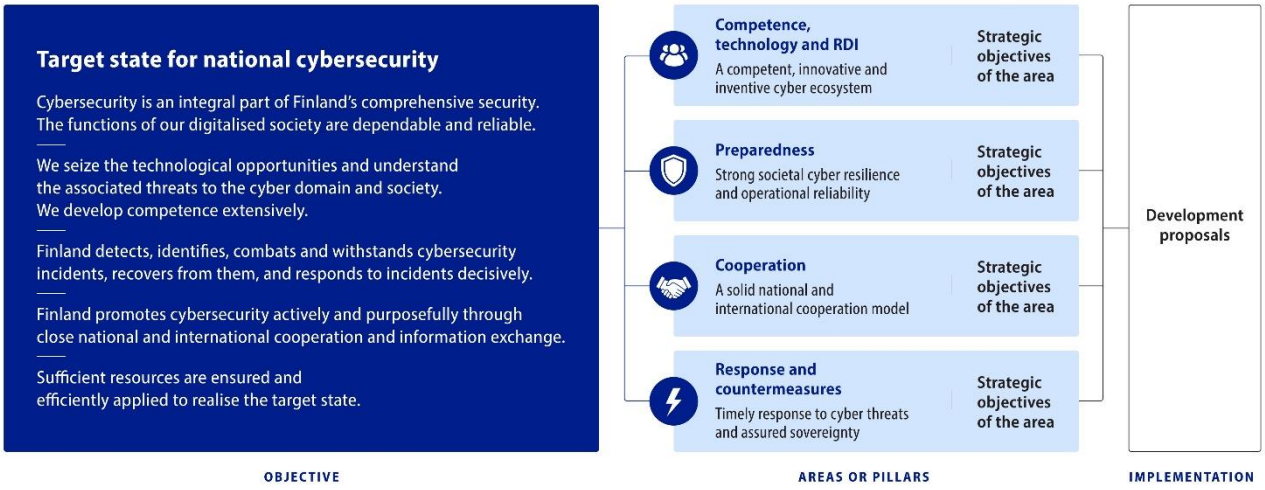
Hundreds of specialists were involved in preparing the strategy and its implementation plan, together with participants from the public and private sectors, the academia and civic organisations. This reflects the commitment of society and the Finnish model of comprehensive security.

The implementation plan sets out measures to achieve the objectives of the cybersecurity strategy. Implementation will be linked to government fiscal planning. The implementation plan will be monitored annually and updated as necessary. The steering group of state secretaries will monitor implementation of the strategy at annual intervals.

The Office of the National Cyber Security Director will bear primary responsibility for coordinating the monitoring, supported by a monitoring group from the ministries and its secretariat. Each administrative branch will be responsible for promoting, financing and reporting on the measures assigned to it.

The overall effectiveness of the implementation plan will be assessed on various metrics, such as national and international cybersecurity performance indicators.

2. Target outcome and structure of the cybersecurity strategy



3. Societal actors engaged in ensuring national cybersecurity

4. Structure of the implementation plan

The implementation plan extends to 2035, and covers all four of the areas or pillars below:

I Competence, technology, and RDI;
II Preparedness;
III Cooperation;
IV Response and countermeasures.

The structure of the implementation plan is linked to the strategic objectives and development proposals set out in these four pillars. These in turn reflect the target outcome for national cybersecurity specified in the strategy.

The measures of the plan have been prioritised under two headings or “baskets”:
Basket 1 includes strategic flagship projects of high or very high impact, with a focus on early implementation.
Basket 2 includes projects of impact currently considered less critical, for implementation in the longer term.

Each measure is described in terms of its objectives, schedule and funding, effectiveness, and the participants involved in its implementation (**main responsible authority** and other actors). The effectiveness of each measure is evaluated in words, and on the scales of national/international and significant/major/very high.

5. Implementation and monitoring of the implementation plan

Implementation of the strategy is monitored nationally on an annual basis. Responsibility for coordinating the monitoring is vested in the Office of the National Cyber Security Director, for which each ministry provides an implementation report. The reporting is coordinated with the government fiscal planning schedule. The Office then compiles a summary of these reports for public authorities and political decision-makers.

On 1 November 2024 the Prime Minister's Office appointed a monitoring group responsible for monitoring implementation of the cybersecurity strategy and assessing its impacts. The monitoring group convenes quarterly, or more often as necessary.

Stakeholders will have the opportunity to take part in evaluating the strategy implementation plan. They will be collectively consulted in the spring, with dialogue actively continuing throughout the year.

The administrative branches plan and set aside the resources required for implementation, and remain responsible for implementing development measures.

The monitoring process reviews how various measures have been implemented compared to the target outcome of the strategy and the development proposals specified in the strategy. Reporting focuses particularly on achievements over the preceding period and the remaining scope for improvement. The process prioritises reporting of concrete results, and it is also important to explain why certain measures have not been taken.

5. Implementation of monitoring of the implementation plan; responsibilities

Steering group of state secretaries (government security management operating model development project)
- Approves the implementation plan
- Annually monitors implementation of the plan (monitoring report)

Office of the National Cyber Security Director
- Coordination of monitoring

- Arranges monitoring group meetings
- Arranges an annual joint event to discuss progress of the implementation plan with stakeholders
- Prepares a monitoring report based on responses from the monitoring group
- Responsible for reporting to the steering group of state secretaries overseeing the government security management operating model development project (VSI OHRY), the ministerial working group on social transformation (YU minry), the Security Committee, and other parties as necessary
- A secretariat for the Cybersecurity strategy monitoring group supports the Office of the National Cyber Security Director in monitoring

Cybersecurity strategy monitoring group

- Prepares and coordinates the implementation plan, updating it as necessary
- Formulates an overview of responses from administrative branches
- Compiles progress information for the monitoring report

Responsible administrative branch/other actor

- Plans and attributes resources
- Develops the cooperation structures that are necessary for its own administrative sector
- Implements development measures, either as the main responsible authority or as a participant
- Reports in its administrative branch, by sector, and to the monitoring group

6. Implementation plan; measures

Pillar I: Competence, technology and RDI
"A competent, innovative and inventive cyber ecosystem"

Measure 1.1.

Developing high-level expertise and work-life skills in the public and private sectors, and the cyber capabilities and preparedness of citizens and civil society

Basket 1

Objectives

- Developing cybersecurity expertise at all educational levels, in liberal adult education, labour force training and continuing education.
- Increasing the effectiveness and availability of training to promote cybersecurity skills at work.
- Enhancing the ability of citizens to act safely.
- Ensuring application and funding of the outcome of the Cyber Citizen project.
- Establishing the conditions for growing excellence through RDI work in the cyber sector.
- Increasing competence and availability in secure software development.
- Applying cyber training from the Finnish Defence Forces and its stakeholders to build up national expertise.

- Developing the use of voluntary national defence.

Timetable and financing

As of 2025
Operating expenses, partly additional resources

Impact assessment and analysis of effectiveness

Improving cybersecurity expertise in society establishes the conditions for societal functionality.

Competence has been improved on three levels: civic skills (including preparedness), general work-life skills and high-level expertise.

Training accommodates expertise requirements, changes in operating conditions and technological breakthroughs.

Effectiveness: national/major.

Responsible and other actors

Ministry of Education and Culture, Ministry of Transport and Communications, Ministry of Defence, Prime Minister's Office, National Emergency Supply Agency, Finnish Transport and Communications Agency Traficom, Finnish Defence Forces, National Defence Training Association of Finland, HAUS Finnish Institute of Public Management, education system actors, business community.

Measure 1.2.

Developing network cooperation in cybersecurity training

Basket 1

Objectives

- Studying a broadening of network cooperation to include vocational education and cooperation with other actors in the sector, based on current cyber competence networks in higher education, led by the University of Jyväskylä and JAMK University of Applied Sciences.

Timetable and financing

2026-2027
Additional resources

Impact assessment and analysis of effectiveness

Improving cooperation between educational actors.

Effectiveness: national/major.

Responsible and other actors

Ministry of Education and Culture

Measure 1.3.

Developing a national capability in cryptographic technology and securing the status of a country that can approve information security products in the EU and NATO cryptographic products

Basket 1

Objectives

- Formulating a national cryptographic technology strategy, implementation programme and management structure.
- Developing an internationally compatible national cryptographic reference architecture and national quantum-secure cryptographic product family.
- Constructing a national cryptographic laboratory.
- Developing security of supply for national encryption solutions.
- Supporting exports of cryptographic products.
- Establishing and expanding a national cryptography training programme and other competence development initiatives.

Timetable and financing

2025-2035
Additional resources

Impact assessment and analysis of effectiveness

Self-sufficiency and security of supply in critical encryption technologies.
Ability of supply-critical actors to secure their own operations from threats to cryptographic solutions.
Export promotion supporting self-sufficiency and security of supply.
Ability to protect critical national information assets in the quantum age.

Effectiveness: national and international/very high.

Responsible and other actors

Ministry of Defence, Ministry of Economic Affairs and Employment, Ministry of Transport and Communications, Finnish Transport and Communications Agency Traficom, Finnish Defence Forces, National Emergency Supply Agency, Business Finland, Finnish Industry Investment - Tesi, Technical Research Centre of Finland - VTT, manufacturing sector, higher education institutions.

Measure 1.4.

National implementation of quantum-secure encryption solutions

Basket 1

Objectives

- Creating a plan and guidelines for transitioning to quantum-safe algorithms while accommodating policies of the national quantum strategy.
- Supporting critical sectors in the quantum transition.
- Assessing the need to impose a duty to use quantum-resistant encryption.
- Applying an innovative public procurement model.

Timetable and financing

2025-2035
Additional resources

Impact assessment and analysis of effectiveness

A timely transition to quantum-secure encryption solutions will prevent confidential information from being compromised, secure the integrity of the data, and ensure that systems and services remain available.

Effectiveness: national/very high.

Responsible and other actors

Ministry of Transport and Communications, Ministry of Economic Affairs and Employment, Ministry of Finance, **Ministry of Defence**, Finnish Defence Forces, Finnish Transport and Communications Agency Traficom, Government ITC Centre Valtori, National Emergency Supply Agency

Measure 1.5.

Basket 1

Anticipating and monitoring the impact on cybersecurity of emerging technologies and phenomena

Objectives

- Establishing a cross-governmental format for future and foresight work in cybersecurity.
- Generating analysed information on future threats and opportunities in cybersecurity for use by public authorities and business, and applying the situational awareness operations of public authorities in information sharing.
- Launching a scenario-based review of the cyber threat landscape in collaboration with public authorities and the business community.

Timetable and financing

As of 2025
Operating expenses

Impact assessment and analysis of effectiveness

Anticipating cybersecurity phenomena can identify needs for future regulation, resourcing and preparedness measures, and support the preparedness of industries and public authorities for cyber threats.

This action is a requirement for preparing the national threat assessment.

Effectiveness: national/very high.

Responsible and other actors

Ministry of Transport and Communications, Prime Minister's Office, other ministries, government agencies, Finnish Transport and Communications Agency Traficom, National Emergency Supply Agency, business community, research institutes

Measure 1.6.

Strengthening the participation of Finnish organisations in cybersecurity funding programmes and expertise network cooperation

Basket 2

Objectives

- Influencing on the work programmes of EU funding programmes and strengthening opportunities for Finnish businesses, universities and research institutes to take part in funding programmes.
- Ensuring sufficient co-financing for participation in projects.
- Promoting the integration of national actors into the EU cybersecurity expertise community, and opportunities for export promotion.
- Maintaining and developing the national education and research community, and helping Finnish actors to find national and international partners for international projects.
- Forming a shared understanding of cybersecurity research field and secure funding

Timetable and financing

2025-2029
Additional resources

Impact assessment and analysis of effectiveness

This measure may promote the development of national cybersecurity innovations, research and expertise.

Improving national uptake of available EU and NATO funding and fostering growth in the cybersecurity sector.

Promoting self-sufficiency in technology.

Strengthening the national cybersecurity ecosystem and its international competitiveness, and improving business and export opportunities for the sector.

Effectiveness: national and international/major.

Responsible and other actors

Ministry of Transport and Communications, Ministry of Defence, **Ministry of Economic Affairs and Employment**, **Ministry of Education and Culture**, **Prime Minister's Office,** Ministry for Foreign Affairs, Finnish Transport and Communications Agency Traficom, National Emergency Supply Agency.

Measure 1.7.

Developing and supporting the national defence industry in innovating and applying defence technologies, emerging and disruptive technologies and dual-use products, and in preparing for threats

Basket 1

Objectives

- Completing and commercialising such initiatives as the secure communication projects of indirect industrial cooperation in the F35 project.
- Establishing the operations of national centres and business accelerators under the NATO DIANA programme on a permanent footing.
- Enhancing the application of EU and NATO development funding.
- Using civilian funding effectively for development of dual-use products.
- Formulating a strategic policy for cyber protection in the defence and security sector and establishing a cybersecurity cooperation network (ISAC).
- Developing common services and response capabilities for the defence and security sector.
- Strengthening Finnish ownership of cybersecurity sector businesses that are critical for the security of supply.

Timetable and financing

As of 2025
Operating expenses, partly additional resources

Impact assessment and analysis of effectiveness

The effectiveness of measures will be assessed through such indicators as:

- the national country profile in emerging and disruptive technologies,

- the national level of RDI funding,
- the utilisation rate of Finnish solutions in critical cutting-edge technology,
- self-sufficiency and impacts on security of supply,
- growth in export potential and export value,
- the application in other countries of solutions that meet international requirements,
- the utilisation rate of national solutions,
- national co-financing (quantity, time), and
- the level of cyber protection in the defence and security sector.

Effectiveness: national and international/very high.

Responsible and other actors

Ministry of Defence, Ministry of Economic Affairs and Employment, Finnish Defence Forces, Technical Research Centre of Finland - VTT, Business Finland, Finnish Industry Investment - Tesi, manufacturing

Measure 1.8.

Developing cybersecurity expertise with organisations and the business community

Basket 1

Objectives

- Launching a joint project with the business community and organisations to promote better citizen cybersecurity skills.
- Improving cooperation between public authorities and organisations in information exchanges and communications concerning threats to citizens and various population groups.
- Supporting the development of cyber capabilities within organisations.
- Boosting the work of the Finnish Safer Internet Centre (FISIC).

Timetable and financing

2025-2027
Operating expenses, partly additional resources

Impact assessment and analysis of effectiveness

The ability of citizens to function safely in society will be strengthened.
They will become less prone to losing money due to scams, with greater confidence in the digital society.

Official cybersecurity advice will be shared through organisations and the business community to strengthen the expertise of the general public. People will know how to prepare for disruptions in a digitalised society.

Effectiveness: national/very high.

Responsible and other actors

Ministry of Transport and Communications, Ministry of Education and Culture, National Audiovisual Institute, Finnish Transport and Communications Agency Traficom**,** National Emergency Supply Agency, business community, organisations

Measure 1.9.

Developing cybercrime prevention training

Basket 2

Objectives

- Developing cybercrime prevention training with respect to cybercrime and cyber-assisted offences. This work will be linked to the previously launched Cyber Capital project and the cyber-assisted crime prevention competence project (Threat Vulnerability Asset TVA methodology).

Timetable and financing

As of 2024
Operating expenses

Impact assessment and analysis of effectiveness

A need for greater competence has been found in the police and other security authorities. Training provided by the Police University College ensures the adequacy of competence in the police, and also supports the operations of other security authorities.

Besides security authorities, public prosecutors, judges and others may also participate in training courses arranged by the Police University College.

Effectiveness: national/major.

Responsible and other actors

Ministry of the Interior, National Police Board, Police University College

Pillar II: Preparedness
“Strong societal cyber resilience and operational reliability”

Measure 2.1.

Compiling a national cyber threat assessment to support preparedness work.

Basket 1

Objectives

Preparing regular national cybersecurity threat assessments based on scenario work for use by public authorities, public administration and the business community.
Increasing the availability and serviceability of national threat assessments.

Timetable and financing

As of 2025
Operating expenses

Impact assessment and analysis of effectiveness

Improving awareness of the cyber threat landscape and phenomena impacting cybersecurity. Improving conditions for preparedness, risk management and criticality classification in different sectors.
Strengthening of the shared cybersecurity situational awareness.
A threat assessment that supports drafting of the national cyber crisis management plan required under the NIS2 Directive, and accommodates the requirements of the CER Directive.

Effectiveness: national/very high.

Responsible and other actors
Ministry of Transport and Communications, Prime Minister's Office, Ministry of the Interior, Ministry of Defence, Finnish Transport and Communications Agency Traficom, Finnish Defence Forces, Finnish Security and Intelligence Service, other public administration, business community, National Emergency Supply Agency

Measure 2.2.

Integrating cyber defence into total defence

Basket 1

Objectives

- Identifying and managing cyber defence linkages with total defence, resilience measures and host nation support.
- Accommodating national defence and military crises in cyber crisis management, and developing preparedness and responses to them in the civilian sector.
- Integrating local cyber defence into local and regional operating models and preparedness.
- Enabling public authorities to support critical actors.
- Improving monitoring of total defence resources with respect to cyber defence.

Timetable and financing

2025-2032
Defence budget
Operating expenses, partly additional resources

Impact assessment and analysis of effectiveness

Enabling Finnish and Allied operations and support for operations.

The necessary response systems have been taken into service, with up-to-date contingency plans and agreements concluded.

The management plan accommodates the military threat and use of military force.

Monitoring resourcing of civil sector public authorities and actors, identifying and managing the risks of resourcing shortfalls as part of total defence management.

Effectiveness: national and international/very high.

Responsible and other actors

Ministry of Defence, Finnish Defence Forces, other administrative branches, civilian sector

Measure 2.3.

Accommodating cybersecurity when drafting new national legislation.

Basket 2

Objectives

Updating impact assessment guidelines for legislative drafting.

Timetable and financing
2025-2027
Operating expenses

Impact assessment and analysis of effectiveness

National legislation accommodates cybersecurity aspects and responds to changes in operating conditions.

The legislative drafting and legislation impact assessments of ministries accommodate cybersecurity aspects.

Effectiveness: national/major.

Responsible and other actors

Ministry of Justice, other ministries

Measure 2.4.

Long-term planning and monitoring of public administration cybersecurity resources.

Basket 2

Objectives

- Planning and monitoring cybersecurity resources for central government, wellbeing services counties and municipalities, and risk-based resource allocation.
- Applying the digital security overview service of the Digital and Population Data Services Agency and other assets.

Timetable and financing

2025-2030
Operating expenses

Impact assessment and analysis of effectiveness

The state of public administration cybersecurity resources must be sufficiently known to ensure their appropriate resourcing and efficient application.

The use of resources in cybersecurity planning is more efficient, for example, by prioritising tasks and guidelines.

Effectiveness will be measured by applying the digital security overview service and the functionality of guidelines.

Effectiveness: national/major.

Responsible and other actors

Ministries, Digital and Population Data Services Agency, other public administration

Measure 2.5.

Ensuring uniform implementation of the Cybersecurity Act

Basket 1

Objectives

- Strengthening cooperation between the Data Protection Ombudsman and public authorities supervising the NIS2 Directive.
- Improving advice and guidance for industries on implementing the National Cybersecurity Act and the Act on Information Management in Public Administration.
- Preparing a national plan for managing major cybersecurity incidents and crises.
- Improving operating conditions for the Data Protection Ombudsman.

Timetable and financing

2025-2029
Operating expenses, partly additional resources

Impact assessment and analysis of effectiveness

The NIS2 Directive is a key cybersecurity statute that harmonises cybersecurity requirements for critical industries and increases national resilience.

Cooperation between supervisory public authorities can harmonise procedures and improve efficiency in applying resources.

Common guidelines can improve and streamline implementation of this legislation within organisations.

Effectiveness: national/very high.

Responsible and other actors

Ministry of Transport and Communications, Ministry of Justice, Ministry of Finance, Finnish Transport and Communications Agency Traficom, Data Protection Ombudsman, public authorities supervising the NIS2 Directive

Measure 2.6.

Actively influencing international cybersecurity standards

Basket 2

Objectives

- Influencing in the cybersecurity standardisation work in international organisations.
- Accelerated implementation of existing standards.
- Developing private sector participation in international standardisation.

Timetable and financing

As of 2025
Operating expenses

Impact assessment and analysis of effectiveness

Ensuring adequate consideration of national aspects in the preparation of standards.
The private sector is prepared and able to apply standards.
Participation in standardisation can be applied starting from RDI phase.

Effectiveness: national and international/major.

Responsible and other actors

Ministry of Transport and Communications, Ministry of Defence, other ministries, Finnish Transport and Communications Agency Traficom, Finnish Defence Forces

Measure 2.7.

Updating legislation on conformity assessment of information systems, services and security-critical products, and developing assessment work concerning the operations of organisations and information systems.

Basket 1

Objectives

- Improving the availability of assessment and official cooperation by revising the assessment functions of public authorities.
- Improving operating conditions for manufacturers of security-critical products and evaluation institutes in accordance with the final working group report.
- Streamlining assessment procedures with risk-based approach, and clarifying and supplementing assessment criteria.
- Developing and harmonising evaluation criteria together with the guidelines and tools, and the technical and automatic methods that support their application.
- Developing the abilities and powers of the Finnish Defence Forces with respect to national and international conformity assessment and approval of their own information systems and encryption solutions.
- Developing certification and essential requirements in the healthcare and social welfare services sector based on the Act on the Processing of Client Data in Healthcare and Social Welfare (703/2023, *Client Data Act*).

Timetable and financing

2024-2027
Operating expenses, partly additional resources

Impact assessment and analysis of effectiveness

Changes in operating conditions necessitate the updating of statutes, reference Ministry of Finance working group report: "Compliance of public administration information systems - status assessment 2024".

The Finnish Defence Forces and Government ITC Centre Valtori have the capacity to conduct independently verified conformity assessments, and the capacity of the private sector to evaluate and support assessments has been improved.

Infrastructure has been constructed to support the assessment and approval of information systems in security-critical sectors. Resourcing needs will be clarified as legislation is prepared.

Effectiveness: national and international/very high.

Responsible and other actors

Ministry of Finance, Ministry of Transport and Communications, Ministry of Defence, Ministry of Social Affairs and Health, other ministries, Finnish Defence Forces, National Cyber Security Director, Finnish Transport and Communications Agency Traficom, Government ITC Centre Valtori, approved evaluation institutions, other public evaluation authorities, other public administration

Measure 2.8.

Developing cybersecurity exercises in response to changed operating conditions in order to increase the resilience of society and ensure operating conditions for total defence.
Basket 1

Objectives

- Ensuring the continuity of KYHA national cybersecurity exercises.
- Diversifying national cyber exercise operations and increasing the number of participants.
- National cyber exercises will meet the needs of total defence.
- Updating exercise scenarios.
- Developing sector-specific and inter-sectoral exercises, including stakeholders.
- Using exercise materials broadly in various industries.
- Developing exercise environments to reflect the cyber threat landscape, including by applying EU funding.
- Also creating training opportunities for the strategic level.
- Participating in multinational (NATO and EU) cyber exercises with the ability to conduct multinational cyber exercises in Finland.

Timetable and financing

2026-2030
Additional resources

Impact assessment and analysis of effectiveness

Versatile exercise activities aimed at both public administration and the private sector strongly promote the cyber resilience and expertise of society.

National preparedness and cyber exercises also support the readiness and development of cyber defence.

Civilian and military actors train together regularly.

Cyber exercises enable the development of cooperation between various levels of operations and public authorities.

Effectiveness: national/very high.

Responsible and other actors

Ministry of Transport and Communications, National Cyber Security Director, National Emergency Supply Agency, Prime Minister's Office, Ministry of Defence, other ministries, Finnish Transport and Communications Agency Traficom, Finnish Defence Forces, Digital and Population Data Services Agency, business community, organisations, National Defence Training Association of Finland in particular

Measure 2.9.

Ensuring the functionality and reparability of the communication connections and data availability required by society, and alternative connection methods where necessary in cases of serious cybersecurity incidents

Basket 1

Objectives

- Verifying international telecommunication connections from the perspective of security of supply.

Timetable and financing

2025-2027
Development implemented as part of the DT2030-programme of the National Emergency Supply Agency.

Impact assessment and analysis of effectiveness

The operation of international telecommunications connections under all conditions is a prerequisite for ensuring security of supply.

Effectiveness: national/very high.

Responsible and other actors

National Emergency Supply Agency, Ministry of Transport and Communications, Finnish Transport and Communications Agency Traficom, business community

Measure 2.10.

Identifying the special cybersecurity needs of various sectors of society, and developing solutions to prepare for and recover from incidents

Basket 1

Objectives

- The continuity, preparedness and contingency procedures of various sectors of society and municipal actors are up-to-date and operational.
- Actors in various sectors of society and the municipal sector may access cyber and digital security training materials that support the expertise of the senior management and staff required for cyber preparedness.

Timetable and financing

2025-2027
Development implemented as part of the DT2030-programme of the National Emergency Supply Agency.

Impact assessment and analysis of effectiveness
All industries rely on digital infrastructure and the services that operate on it. Operations will seek to improve sector-specific cybersecurity in sectors that are critical to security of supply.

Effectiveness: national/very high.

Responsible and other actors

National Emergency Supply Agency, Finnish Transport and Communications Agency Traficom, business community

Measure 2.11.

Maintaining and supporting the ability of digital infrastructure providers to prepare for serious cyber incidents

Basket 2

Objectives

- Supporting the ability of telecommunication operators and digital infrastructure providers to prepare for cyber threats in changed operating conditions.
- Promoting cooperation between public authorities and telecommunication operators on issues of mobile network development.

Timetable and financing

As of 2024
Operating expenses

Impact assessment and analysis of effectiveness

Timely and confidential collaboration can improve the preparedness of digital infrastructure actors for cyber threats and technological disruption.

Collaboration can proactively identify and prevent security threats arising from new communication technologies, and lobby for reinforced security of the communications infrastructure through international cooperation.

Effectiveness: national/major.

Responsible and other actors

Ministry of Transport and Communications, Finnish Transport and Communications Agency Traficom, National Emergency Supply Agency

Measure 2.12.

Improving the resilience of terrestrial systems through space services

Basket 2

Objectives

- Recognising the dependency of critical societal infrastructure on space services.
- Ensuring the availability of radio frequencies for Finnish ground station and satellite business operations.
- Improving the resilience of terrestrial systems by using space services as backup systems in communication and time synchronisation.
- Securing international supply chains for space services and reinforcing Finnish ownership of national actors.
- Commissioning certified satellite services provided by the EU Space Programme for public authorities and critical infrastructure at suitable locations.
- Monitoring cybersecurity as part of the space situational awareness in partnership with various actors.
- Considering the cybersecurity of space systems in permits, licensing conditions and system lifecycle management.

Timetable and financing

Operating expenses, 2025–2030

Impact assessment and analysis of effectiveness

The availability and continuity of space services will improve. Critical infrastructure will be able to rely on space services while remaining prepared for disruptions in such services.

Effectiveness: national and international/very high.

Responsible and other actors

Ministry of Transport and Communications, Ministry of Economic Affairs and Employment, Ministry of the Interior, Prime Minister’s Office, National Emergency Supply Agency, Finnish Transport and Communications Agency Traficom

Measure 2.13.

Improving the security of hardware and software by ensuring smooth and effective implementation of the EU Cyber Resilience Act (CRA)

Basket 1

Objectives

- Promoting market access and competition in the EU internal market for manufacturers of devices and software incorporating a digital element.
- Ensuring that public authorities can smoothly approve a sufficient number of notified bodies performing third-party assessment, and thereby prevent bottlenecks in market entry.
- Promoting a level of information security of hardware and software by guiding enterprises with respect to new requirements, and by arranging their market surveillance appropriately and smoothly.
- Ensuring the ability of the National Cyber Security Centre to coordinate notifications of hardware and software vulnerabilities, as required under the Regulation.
- Supporting the functions of the competent authority for cybersecurity certification as implementation of the Cyber Resilience Act increases the demand for certification.

Timetable and financing

2026–2030

Operating expenses, partly additional resources

Impact assessment and analysis of effectiveness

The Cyber Resilience Act is a key new EU Regulation imposing minimum security requirements on hardware and software that can be connected to the Internet or to another device. Phased application of the Regulation will begin in 2026–2027. Successful implementation of the regulation has significant importance for equipment security and the secure use of software; and for the competitiveness of Finnish companies; i.e. how equipment and software manufactures can enter the EU market and compete in the internal market.
The Regulation will ensure that products have fewer vulnerabilities, and that manufacturers remain responsible for cybersecurity throughout the entire life cycle of a product.

Effectiveness: national and international/very high.

Responsible and other actors

Ministry of Transport and Communications, Finnish Transport and Communications Agency Traficom

Pillar III: Cooperation
"A solid national and international collaboration model"

Measure 3.1.

Developing harmonisation of national cyber policy objectives to promote Finland's international profile and increase effectiveness

Basket 1

Objectives

- Developing the active participation of Finland in key bilateral and multilateral networks and cooperation, and actively influencing in international organisations, especially in the EU and NATO.
- Creating a national coordination format for international collaboration in cybersecurity and cyber defence.
- Implementing active strategic and operational cooperation with key countries.
- Lobbying to accommodate cybersecurity aspects in EU provisions and international agreements.
- Seeking to promote the Finnish cooperation model based on comprehensive security and preparedness internationally.

Timetable and financing
As of 2024
Operating expenses

Impact assessment and analysis of effectiveness

Finland has achieved the critical objectives that it assigned in the international context.
The necessary arrangements and agreements have been made, and strategic and operational cooperation has begun.

EU-NATO cooperation supports the cybersecurity and cyber defence of Finland. A national situational awareness and harmonisation format for international cyber policy has been created and established.

Finland has actively encouraged the development of priorities and principal functions of EU-NATO cooperation in a direction that supports national cybersecurity and cyber defence.

Effectiveness: national and international/very high.

Responsible and other actors

Ministry for Foreign Affairs, Prime Minister's Office, National Cyber Security Director, Ministry of Defence, Ministry of Transport and Communications, Finnish Transport and Communications Agency Traficom, Finnish Defence Forces

Measure 3.2.

Developing the security of international health data exchange

Basket 1

Objectives

- Conducting a risk assessment in the course of preparing and completing implementation of the European Health Data Space / primary and secondary use of social welfare and health data.

Timetable and financing

2025-2031
Operating expenses

Impact assessment and analysis of effectiveness

Ensuring that the national level of cybersecurity satisfies EU information exchange operating conditions.

Effectiveness: national and international/very high.

Responsible and other actors

Ministry of Social Affairs and Health, Social Insurance Institution (Kela), National Institute for Health and Welfare (THL), National Supervisory Authority for Welfare and Health (Valvira)

Measure 3.3.

Implementing the measures of the report on the authorities' capacity to act in cyber security matters insofar as these are not covered by other measures.

Basket 1

Objectives

- Improving cooperation, processes and information exchange between public authorities and the private sector, e.g. in preparedness, response andlegislation.
- Identifying entities and their supply chains providing vital functions for society.
- Updating the Vocabulary of Cyber Security.
- Considering the cyber operating environment in preparedness legislation and amending legislation to enable assistance to critical entities
- Developing joint technical solutions for exchanging highly classified information.

Timetable and financing

2025-2030
Additional resources in part

Impact assessment and analysis of effectiveness

Enabling efficient cooperation in public administration using advanced solutions for handling classified and sensitive information.

Effectiveness: national and international/very high.

Responsible and other actors

Ministry of the Interior, Ministry of Defence, Ministry for Foreign Affairs, Ministry of Finance, **Ministry of Transport and Communications, National Cyber Security** Director, Prime Minister's Office, Ministry of Justice, Finnish Transport and Communications Agency Traficom, Finnish Defence Forces, Government ITC Centre Valtori, National Bureau of Investigation, Finnish Security and Intelligence Service

Measure 3.4.

Clarifying responsibilities in developing national cyber defence

Basket 1

Objectives

- Describing an operating model for national cyber defence cooperation in the cyber defence doctrine.
- An operational cooperation structure of public authorities enables coordination of operational cooperation between public authorities, including cyber defence functions in all states of readiness.
- Enhancing cooperation, information exchange and response, accommodating the needs arising between various sectors, including legislation: civil-military cooperation, cooperation between public authorities and the private sector, cooperation between the defence and security sectors, and cooperation in voluntary national defence.

Timetable and financing

2025-2032
Additional resources

Impact assessment and analysis of effectiveness

Collaboration structures are formed and operational at various levels, and there is a development plan.

Collaboration has been developed to support cyber situational awareness and implementation of actions (including countermeasures).

Cyber defence is able to support other authorities and sectors in a coordinated manner with information and capabilities.

Finland presents itself as a unified operator in cyber defence.

Effectiveness: national and international/very high.

Responsible and other actors

Ministry of Defence, Finnish Defence Forces, other ministries and public authorities, National Emergency Supply Agency, business community, organisations

Measure 3.5.

Ensuring easy availability of up-to-date cybersecurity guidance for public administration, businesses, citizens and organisations

Basket 2

Objectives

- Creating and maintaining a national database and service catalogue of cybersecurity guidance, including guidelines for social welfare and health care.
- Collecting good practices for implementing cybersecurity in public administration and sharing them for shared use through a common channel.

Timetable and financing

2024-2028
Operating expenses

Impact assessment and analysis of effectiveness

A common guidance database will enhance efforts to improve cybersecurity and cooperation in society.

Effectiveness: national/major.

Responsible and other actors

Ministry of Finance, Ministry of Social Affairs and Health, Digital and Population Data Services Agency

Measure 3.6.

Developing formulation and sharing of situational awareness and strengthening situational awareness in various organisations

Basket 1

Objectives

- Developing formulation of strategic situational awareness to serve the needs of target groups, with transmission of information on cybersecurity incidents to the Government Situation Centre.
- Ensuring the continuity of National Cyber Security Centre's situational awareness products and their availability to the correct target groups.
- Developing cooperation network operations to reflect changed operating conditions with safeguarding of network operations.
- Enhancing cooperation and joint incident management between supervisory authorities (NIS2) and the Data Protection Ombudsman.

Timetable and financing

2025-2027
Additional resources

Impact assessment and analysis of effectiveness

Reviewing target groups ensures the availability of timely situational awareness products widely in society.

Effectiveness: national/very high.

Responsible and other actors

Ministry of Transport and Communications, **Prime Minister's Office,** Finnish Transport and Communications Agency Traficom, Data Protection Ombudsman, other public administration

Measure 3.7.

The public and private sectors together develop and provide centralised cybersecurity services

Basket 1

Objectives

- Ensuring the continuity of services provided by the Traficom's National Cyber Security Centre and broadening the use of services such as Cybermeter and Hyöky (national attack surface mapping) to include wider target groups.
- Strengthening the effectiveness of the VAHTI digital security development network, Taisto digital security preparedness exercises and Julkri (data security evaluation criteria for public administration) tool provided by the Digital and Population Data Services Agency.
- Increasing the utilisation rate, effectiveness and application of the administrative digital security situation picture service provided by Digital and Population Data Services Agency for public administration.

- Formulating templates and negotiating agreements centrally.
- Identifying and developing new services where required.

Timetable and financing

2024-2030
Operating expenses, partly additional resources

Impact assessment and analysis of effectiveness

Common centralised cybersecurity services will intensify use of resources. The widespread use of the services is necessary for significantly improving the security and functional reliability of public services. Ensuring the continuity of services, new services and service expansions will require additional resources.

Effectiveness: national/very high.

Responsible and other actors

Ministry of Transport and Communications, **Ministry of Finance,** National Emergency Supply Agency, Finnish Transport and Communications Agency Traficom, Digital and Population Data Services Agency, public administration ICT companies, private sector, other public administration

Measure 3.8.

Enhancing the security and functional reliability of shared information and communication technology services and information assets

Basket 1

Objectives

- Implementing a security development programme for shared information and communication technology services (PATO).
- Securing critical data repositories and critical site location information.
- Ensuring operational information exchange and management through a common secure information exchange solution to guarantee critical communications.

Timetable and financing

2024-2030
Operating expenses

Impact assessment and analysis of effectiveness

Reliable shared information and communication technology services support the smooth functioning of society, enabling efficient implementation of strategic functions.

Effectiveness: national/very high.

Responsible and other actors

Ministry of Finance, Government ITC Centre Valtori, Erillisverkot Group

Measure 3.9.

Revising the legislation on the security network and shared information and communication technology services.

Basket 2

Objectives

- Enabling the use of authorities' cyber capabilities by regulation and agreements for protecting the providing of the shared information and communication technology services for central government.

Timetable and financing

2026-2029
Operating expenses

Impact assessment and analysis of effectiveness

Optimally efficient use of public authority resources in providing shared information and communication technology services, and in protecting strategic functions in accordance with the Security Strategy for Society.

Effectiveness: national/major.

Responsible and other actors

Ministry of Finance, Ministry of Defence, Finnish Defence Forces, Government ITC Centre Valtori

Measure 3.10.

Clarifying the needs to improve security classification legislation

Basket 1

Objectives

- Clarifying the suitability of security classification regulations, having regard to cloud services and artificial intelligence, and implementing the necessary statutory amendments.
- Studying the scope of the duty of security classification and clarifying guidelines, especially in wellbeing services counties, municipalities and special assignment companies, and amending legislation where required.

- Reviewing compatibility with international provisions in the course of any statutory amendments.

Timetable and financing

2025-2029
Operating expenses

Impact assessment and analysis of effectiveness

Up-to-date security classification provisions coupled with an appropriate scope and guidelines will enhance national cybersecurity.

Effectiveness: national/major.

Responsible and other actors

Ministry of Finance, Ministry for Foreign Affairs

Pillar IV: Response and countermeasures "Timely responses to cyber threats and assured sovereignty"

Measure 4.1.

Developing the readiness and ability of wellbeing services counties to prepare for cyber incidents and respond to them in a timely manner

Basket 2

Objectives

- Wellbeing services counties applying a uniform criticality classification to classify their key information systems and functions.
- Clarifying incident reporting procedures in wellbeing services counties.
- Reinforcing the cooperation network between preparedness centres for healthcare and social welfare (5) and national actors, with deployment of a new risk management model for wellbeing services counties to improve ICT incident management.
- Ensuring the security of national social welfare and healthcare services.

Timetable and financing

2024-2030
Operating expenses, partly additional resources
Development also implemented as part of the DT2030-programme of the National Emergency Supply Agency.

Impact assessment and analysis of effectiveness

An improved ability of wellbeing services counties to prepare for and respond to cyber threats in their operating environment.
Maintained awareness of cybersecurity as part of developing the operations of social welfare and healthcare organisations.

Effectiveness: national/major.

Responsible and other actors

Ministry of Social Affairs and Health, Ministry of Justice, Ministry of Finance, Ministry of the Interior, wellbeing services counties, Finnish Transport and Communications Agency Traficom, National Supervisory Authority for Welfare and Health (Valvira), Data Protection Ombudsman, business community

Measure 4.2.

Developing the readiness and ability of municipalities to prepare for cyber incidents and respond to them in a timely manner

Basket 2

Objectives

- Reinforcing risk management, continuous improvement, a safety culture and sharing of best practices, including a Virtual Incident Response Team (VIRT), ICT preparedness, incident management, secure procurement and security of cloud services in applicable national, regional and local inter-municipal networks.
- Maintaining and developing essential national information security and data protection networks to enable peer-to-peer networking and information sharing between organisations.
- Municipalities implement a criticality classification of key information systems and functions.

Timetable and financing

2024-2030
Operating expenses
Development also implemented as part of the DT2030-programme of the National Emergency Supply Agency.

Impact assessment and analysis of effectiveness

Improving the ability of municipalities to prepare for and respond to cyber threats in their operating environment.

Effectiveness: national/significant.

Responsible and other actors

Ministry of Finance, municipalities, Digital and Population Data Services Agency, Finnish Transport and Communications Agency Traficom, other public administration, business community

Measure 4.3.

Reinforcing the preparedness and response of critical industries to cyber incidents

Basket 2

Objectives

- Supporting critical industries in preparing for and responding to cyber incidents and personal data breaches, including by applying the EU cybersecurity emergency mechanism.
- Promoting the participation of Finnish managed security service providers in the EU cybersecurity reserve.
- Using the services of the EU cybersecurity reserve in response to significant or major incidents.
- Improving operating conditions for the Data Protection Ombudsman.

Timetable and financing

As of 2025
Additional resources in part

Impact assessment and analysis of effectiveness

Enabling or accelerating the implementation of measures to improve cybersecurity in organisations, and thereby improving their readiness and ability to prepare for cybersecurity incidents and respond to them in a timely manner.

EU-funded preparedness measures require 50 per cent national co-financing.

Effectiveness: national/major.

Responsible and other actors

Ministry of Transport and Communications, Ministry of Justice, Finnish Transport and Communications Agency Traficom, Data Protection Ombudsman

Measure 4.4.

Ensuring a national detection capacity (the HAVARO service)

Basket 1

Objectives

- Ensuring the operation and continuity of the HAVARO service. (HAVARO = national monitoring and early warning system for serious information security threats).
- Promoting the use of HAVARO in securing the vital functions of society.

Timetable and financing

2026-2030
Additional resources

Impact assessment and analysis of effectiveness

The HAVARO service provides information enabling user organisations to build and develop their own cyber protection.

Securing the continuity of HAVARO will ensure a national cyber threat detection capacity and maintain national cybersecurity.

Effectiveness: national/very high.

Responsible and other actors

Ministry of Transport and Communications, Finnish Transport and Communications Agency Traficom, National Emergency Supply Agency

Measure 4.5.

Ensuring sufficient intelligence collection capability for intelligence agencies

Basket 2

Objectives

- Developing the capability and ensuring the resources to detect state-sponsored cyber espionage and influencing.
- Developing cyber intelligence in response to evolving operating conditions.

Timetable and financing

2025-2035
Additional resources

Impact assessment and analysis of effectiveness

Cyber espionage detection is crucial for identifying the threats and limiting their impacts.

Effectiveness: national and international/major.

Responsible and other actors

Ministry of the Interior, **Ministry of Defence,** Finnish Defence Forces, Finnish Security and Intelligence Service

Measure 4.6.

Developing cooperation between public authorities, enhancing situational awareness and threat detection, and strengthening participation in international cooperation

Basket 2

Objectives

- Strengthening national cooperation between public authorities, cyber situational awareness and cyber threat detection capabilities by applying funding through the EU Cybersecurity Alert System.
- Strengthening international cooperation by participating in cross-border situational awareness cooperation in accordance with the Cyber Solidarity Act.
- Creating a national cybersecurity hub at the Traficom's National Cyber Security Centre to participate in cross-border cooperation and enhance the sharing of national situational awareness and threat information.

Timetable and financing

2025-2032
Additional resources in part

Impact assessment and analysis of effectiveness

Effective threat detection and shared situational awareness can prevent cyber incidents and reduce their impact.

Participating in joint procurement of EU-level situational awareness and detection capabilities can lead to cost savings, enhance cyber threat intelligence (CTI) collection and accelerate threat detection with EU member states.

Effectiveness: national and international/major.

Responsible and other actors

Ministry of Transport and Communications, Prime Minister's Office, Ministry of Defence, Ministry of the Interior, Finnish Transport and Communications Agency Traficom, Finnish Defence Forces, other security authorities

Measure 4.7.

Ensuring resources for combating serious and organised cybercrime and cyber-assisted crimes and for cyber defence

Basket 1

Objectives

- Ensuring and developing the capacity for crime prevention and investigation, and realising criminal liability.
- Developing cooperation between crime prevention and cyber defence, especially in cases involving state-sponsored actors.

Timetable and financing

As of 2024
Operating expenses

Impact assessment and analysis of effectiveness

To realise criminal liability and the smooth functioning of society, it is important for the police to have sufficient capability to investigate cases of serious and organised cybercrime, and to provide support for the work of law enforcement authorities in other countries.

A corresponding capability is necessary for discharging the cyber defence functions of the Finnish Defence Forces, and to the extent stipulated in the Act on Military Discipline and Combating Crime in the Defence Forces.

Effectiveness: national and international/very high.

Responsible and other actors

Ministry of the Interior, Ministry of Defence, National Police Board

Measure 4.8.

Establishing international crime prevention cooperation in combating cybercrime (J-CAT)

Basket 2

Objectives

- Establishing international operations in combating cybercrime. Ensuring operational cooperation capable of combating serious and organised international crime.

Timetable and financing

As of 2024
Operating expenses

Impact assessment and analysis of effectiveness

Serious cybercrime is international by definition, with J-CAT cooperation demonstrating that international operational work is essential and providing a functional platform for this work.

Effectiveness: national and international/major.

Responsible and other actors

Ministry of the Interior, National Police Board, National Bureau of Investigation

Measure 4.9.

Intensifying cooperation between public authorities to improve cybercrime situational awareness and prevent cyber-enabled crime

Basket 2

Objectives

- Studying the most typical ways of committing (cyber) offences, their prevalence, good practice in preventing them, and the criminal damage that they cause.
- Influencing in identified threats and perpetrators based on situational awareness.
- Educating the public through good practices.
- Developing multi-agency cooperation and collaboration with online traders (business community) to combat online shopping fraud.

Timetable and financing

As of 2025
Operating expenses

Impact assessment and analysis of effectiveness

Improving situational awareness on cyber-enabled crime and using this as a basis to help prevent the most typical ways of committing offences.

Effectiveness: national/major.

Responsible and other actors

Ministry of Justice, Ministry of the Interior, Ministry of Economic Affairs and Employment, National Council for Crime, Police, Finnish Transport and Communications Agency Traficom, Finnish Competition and Consumer Authority, Consumer Ombudsman, Data Protection Ombudsman

Measure 4.10.

Preparing a national attribution framework

Basket 1

Objectives

- Creating a national attribution framework.
- Clarifying processes, and the roles and responsibilities of public authorities (technical, operational and political).

Timetable and financing

As of 2024
Operating expenses

Impact assessment and analysis of effectiveness

The attribution framework enhances the effectiveness of Finnish foreign and security policy, for example by developing response capabilities to hostile cyber activities and promoting rules-based and responsible state behaviour in the cyber environment.
The attribution framework develops an ability and readiness to attribute cyber threat incidents targeting Finland, and to demonstrate support for international organisations and partners.

Effectiveness: national and international/very high.

Responsible and other actors

Ministry for Foreign Affairs, Prime Minister's Office**,** Ministry of the Interior, Ministry of Defence, Ministry of Transport and Communications, National Cyber Security Director, Office of the President of the Republic of Finland, intelligence authorities, Finnish Transport and Communications Agency Traficom, Finnish Defence Forces, National Bureau of Investigation

Measure 4.11.

Preparing a cyber defence doctrine

Basket 1

Objectives

- Preparing and adopting the doctrine.
- Identifying and clarifying the processes and the roles and responsibilities of different public authorities in cyber defence.
- Describing the principles of monitoring, protecting and safeguarding state sovereignty.
- Updating the Government resolution on the application of international law.
- Developing the basis for assessing the effectiveness of cyber countermeasures and operations on both strategic and operational level.

Timetable and financing

2024-2026
Operating expenses

Impact assessment and analysis of effectiveness

The cyber defence doctrine will create the capability for a comprehensive and coordinated response and countermeasures to hostile activity.

Developing cooperation and goal awareness.

Developing the capability to support allies and to apply their capabilities in national cyber defence.

Effectiveness: national and international/very high.

Responsible and other actors

Ministry of Defence, **Ministry for Foreign Affairs,** Prime Minister's Office, Ministry of the Interior, Ministry of Transport and Communications, Office of the President of the Republic of Finland, Finnish Defence Forces, National Cyber Security Director, Finnish Transport and Communications Agency Traficom, Finnish Security and Intelligence Service, Police

Measure 4.12.

Developing national and military cyber defence and completing their integration into NATO

Basket 1

Objectives

- Updating the statutory basis for cyber defence duties and powers.
- Updating the statutory basis for safeguarding state sovereignty.
- Continuing development of cyber defence capabilities nationally, operationally and locally.
- Enabling flexible support to other authorities and similar support between various public authorities.
- Completing integration of total defence and the defence system with respect to cybersecurity.
- National resilience work realised, incorporated into preparedness plans, and practised.

Timetable and financing

2024-2032
Additional resources in part

Impact assessment and analysis of effectiveness

Securing state sovereignty.

Creating the capability for a national comprehensive and coordinated response and countermeasures.

Finland is able to operate as part of the alliance, and of its deterrence and defence, including the cyber domain.

Finland can render and receive assistance.

Finland can support allied forces operating in the region, including in a contested cyber environment.

Effectiveness: national and international/very high.

Responsible and other actors

Ministry of Defence, Finnish Defence Forces, Ministry for Foreign Affairs, Ministry of Transport and Communications, Ministry of the Interior, other ministries, other public authorities and municipal and regional actors, critical enterprise sector

Measures

Finland produces information for international cybersecurity index surveys (International Telecommunication Union ITU Global Cyber Index GCI and e-Governance Academy National Cyber Security Index NCSI).

Objectives

- Finland ranks among leading countries in international index measurements.

Timetable and financing

As of 2026
Operating expenses

Impact assessment and analysis of effectiveness

Indicators are used to support national development work.

Effectiveness: national/very high.

Responsible and other actors

National Cyber Security Director, strategy monitoring group