



Overview of the Common Cybersecurity Standards for Critical Infrastructure

(Common Standards for Cybersecurity Measures for Critical Infrastructure)

July 31, 2026

National Cybersecurity Office (NCO), Cabinet Secretariat

※Partially Updated in October 2026

Enhancement of Public Private Partnership

- ❑ Mandatory Measures for Specified Essential Infrastructure Service Providers
 - Registration of covered critical computing devices
 - Incident reporting
- ❑ Establishment of the Collaborative Council for Information Sharing and Measures
- ❑ Enhancement of Vulnerability Response Capability

Utilizing Communications Data

- ❑ Obtaining communications data based on agreements with users such as Specified Essential Infrastructure Service Providers
- ❑ Obtaining communications data without consents
- ❑ Automated screening of “machine-related data”
- ❑ Cooperation with relevant government agencies in analysis
- ❑ Strict handling of obtained communications data
- ❑ Preliminary review and continual inspections after the approval by the independent authority

Remote Access and Neutralization Measures

- ❑ Remote access measures by the police to prevent the serious danger
- ❑ Requirement of Pre-Approval by the Independent Authority and the Commissioner-General or Prefectures’ Chiefs’ direction
【Amendment of the Police Duties Execution Act】
- ❑ Critical computing systems protection measures operated by JSDF by the order of the Prime Minister (PM)
(The Police Duties Execution Act shall apply mutatis mutandis to the execution of duties of JSDF)
- ❑ Protections of computers used by the JSDF and the U.S. military in Japan
(The Police Duties Execution Act shall apply mutatis mutandis to the execution of duties of JSDF)
【Amendment of the Self-Defense Forces Law】

└─❑ Generating and Providing Comprehensive Analyses─┐

Organizational and Structural Development

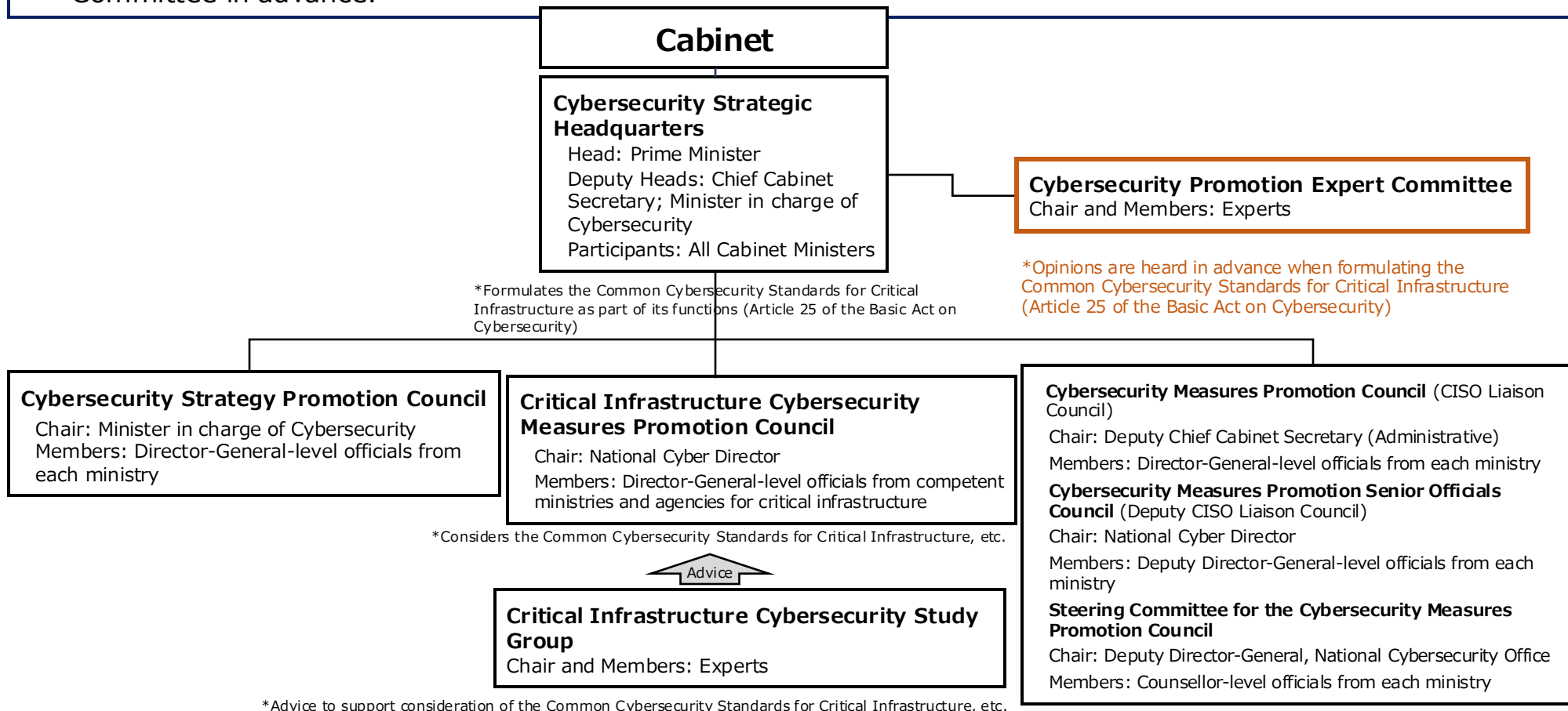
- ❑ Restructuring the Cybersecurity Strategic Headquarters
- ❑ Enhancing the functions of the Cybersecurity Strategic Headquarters
(Amendment to the Basic Act on Cybersecurity)
- ❑ Appointment of National Cyber Director

Development of Common Cybersecurity Standards for Critical Infrastructure, etc.

Date of Enforcement

The date of enforcement will be specified within a period not exceeding one year and six months from the day of promulgation by a Cabinet Order.

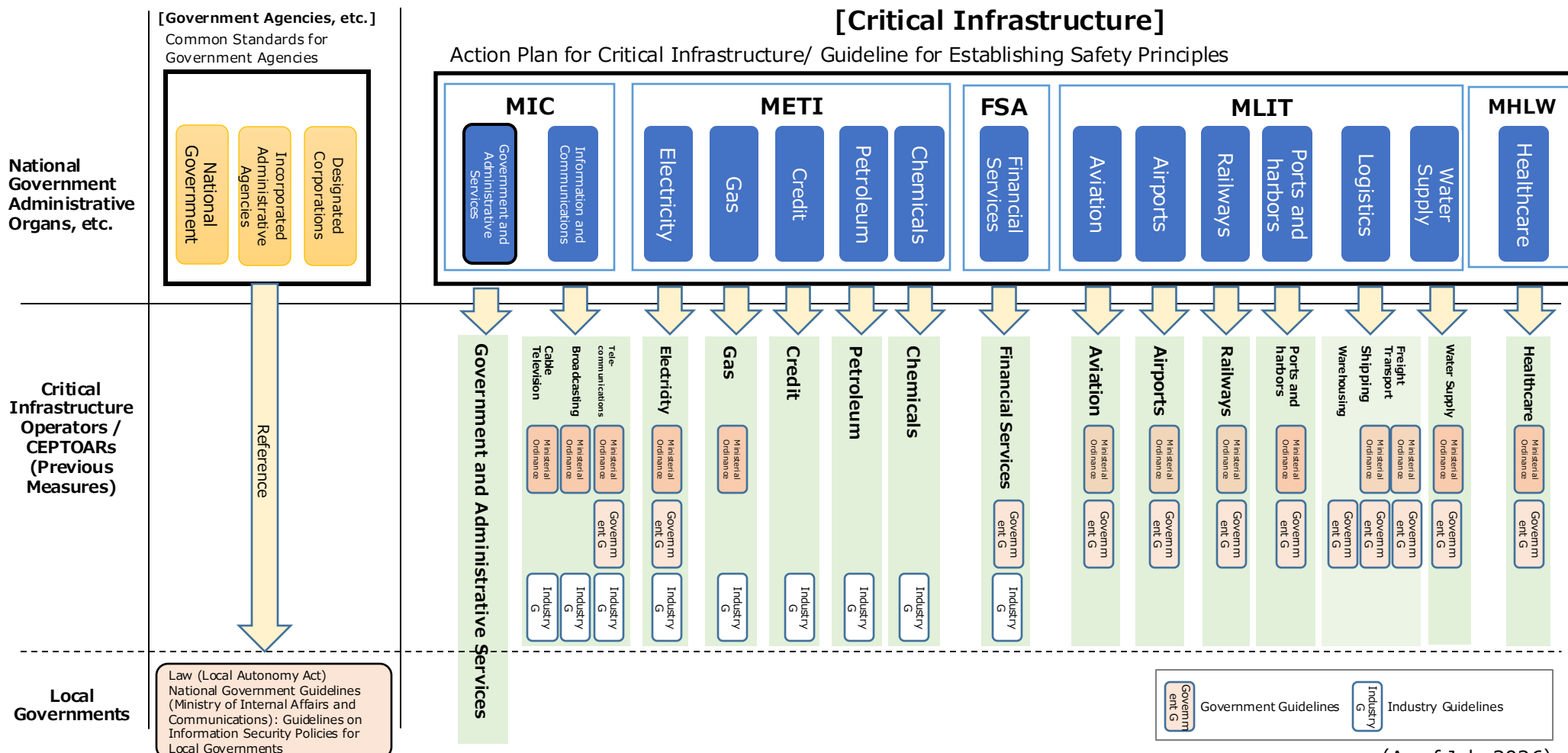
- Following amendments to the Basic Act on Cybersecurity and other legislation, the **Critical Infrastructure Cybersecurity Measures Promotion Council**, established under the Cybersecurity Strategic Headquarters, has been considering the Common Cybersecurity Standards for Critical Infrastructure, etc. (since August 2025).
- To obtain the knowledge and insights of private-sector experts for these deliberations, the **Critical Infrastructure Cybersecurity Study Group** has been convened as a private advisory group to the National Cyber Director (since November 2025).
- In addition, when formulating the Common Cybersecurity Standards for Critical Infrastructure, the Cybersecurity Strategic Headquarters is required to hear the opinions of the Cybersecurity Promotion Expert Committee in advance.



Issue (1) (Variations Across Sectors and Operators)

3

- In each sector, standards and guidelines have been established by the government and industry associations based on the Action Plan, and efforts are underway to ensure cybersecurity. However, **the content and level of these measures vary across sectors and operators.**
- To address increasingly sophisticated and advanced cyber threats, critical infrastructure operators, etc. need to **thoroughly implement baseline cybersecurity measures that should be taken across sectors and operators.**



(As of July 2026)

Issue (2) (Identification of Critical Infrastructure Operators) 4

- The Common Cybersecurity Standards for Critical Infrastructure will ensure the effectiveness of cybersecurity enhancement by promoting their incorporation into sector-specific standards and guidelines and into initiatives by critical infrastructure operators, etc., **while evaluating and improving measures by relevant ministries and agencies and initiatives by critical infrastructure operators, etc.** (PDCA cycle).
- In doing so, **the sectors and operators subject to the standards need to be identified** in the Common Cybersecurity Standards for Critical Infrastructure.

■ Identification of Critical Infrastructure Sectors, etc. under the Action Plan (Previous)

- Critical infrastructure sectors are identified in the Appendix to the Action Plan.

(Examples)

Critical Infrastructure Sector	Critical Infrastructure Operators, etc. Covered	Examples of Critical Systems Covered
Information and Communications	• Major telecommunications operators • Major terrestrial base broadcast operators • Major cable television operators	• Network systems • Operations support systems • Organization/operation systems
Electricity	• General transmission and distribution operators, major power generation operators, etc.	• Electric Power control systems • Smart meter systems
Healthcare	• Medical facilities (excluding small-scale facilities)	• Medical examination record management systems, etc. • Medical examination support systems • Community medical care support systems

- Specific critical infrastructure operators (by name) are identified by competent ministries and agencies for critical infrastructure.

Both the critical infrastructure sectors and specific operators (by name) need to be identified in the Common Cybersecurity Standards for Critical Infrastructure.

Issue (3) (Critical Infrastructure and Essential Infrastructure)⁵

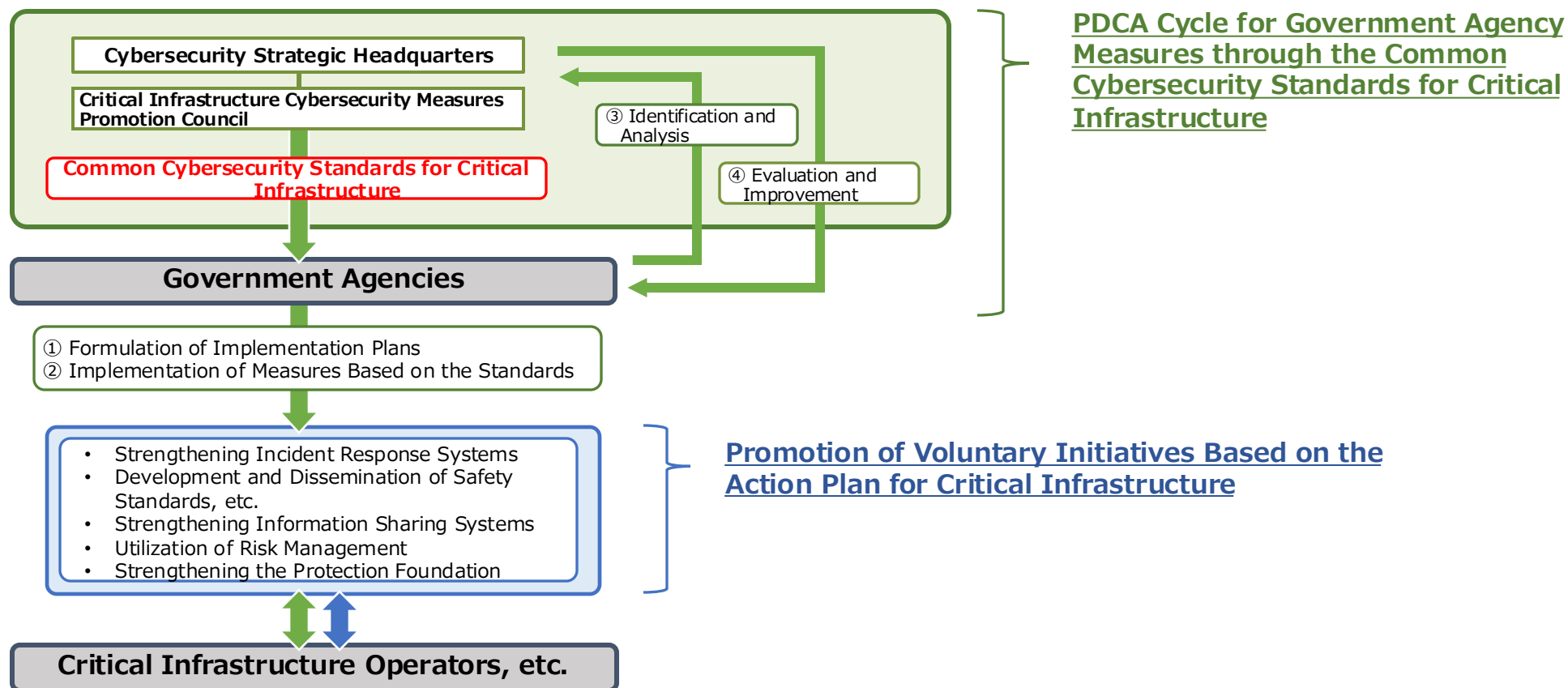
- The scope of critical infrastructure operators, etc. and essential infrastructure service providers is **defined based on the purpose of the respective acts, and differs between the two**. From the perspective of ensuring cybersecurity, it is important, for example, to newly designate sectors and operators have traditionally been classified as essential infrastructure but not as critical infrastructure as critical infrastructure sectors and operators, and **require thorough implementation of baseline cybersecurity measures that should be taken across sectors and operators, including essential infrastructure service providers**.

Critical Infrastructure		Essential Infrastructure	
Electricity	(General electricity transmission and distribution services , power generation services)	Electricity	(General electricity transmission and distribution services, electricity transmission services, electricity distribution services, etc.)
Gas	(General gas pipeline services, gas manufacturing services)	Gas	(General gas pipeline services, specified gas pipeline services, gas manufacturing services)
Petroleum	(Petroleum supply)	Petroleum	(Petroleum refining services, petroleum gas import services)
Water Supply	(Supply of water through water services)	Water Supply	(Water supply services other than small-scale water supply services, wholesale water supply services)
Railways	(Passenger transportation services, ticketing, entry and exit procedures)	Railways	(Type I railway services)
Logistics	(Motor truck transportation services, shipping services, warehousing services)	Truck transport	(General motor truck transportation services)
		International Maritime Cargo	(Scheduled cargo shipping services, non-scheduled shipping services)
Ports and harbors	(Terminal operations using TOS)	Port and Harbor Transport	(General port transportation services)
Aviation	(Air transportation services for passengers and cargo, reservations, ticketing, boarding/loading procedures, flight maintenance, flight planning)	Air Transport	(Domestic scheduled air transportation services, international air transportation services)
Airports	(Ensuring airport security, improving convenience at airports)	Airports	(Services involving the establishment and management of airports, public facility management services related to airports)
Information and Communications	(Telecommunications, broadcasting, cable television)	Telecommunications	(Telecommunications services requiring registration, telecommunications services requiring notification)
		Broadcasting	(Terrestrial basic broadcasting)
—	—	Postal Service	(Postal services)
Financial Services	(Banks, life insurance, non-life insurance, etc.)	Financial Services	(Banks, life insurance, non-life insurance, etc.)
Credit	(Credit services)	Credit Cards	(Business providing comprehensive credit purchase intermediation services)
Healthcare	(Medical examination)	Healthcare	(Note) On June 17, 2026, an amendment adding the healthcare sector was promulgated. The amendment will take effect on a date specified by Cabinet Order within a period not exceeding one year and six months from the date of promulgation.
Chemicals	(Petrochemical industries)	—	—
Government and Administrative Services	(Local government administration services)	—	—

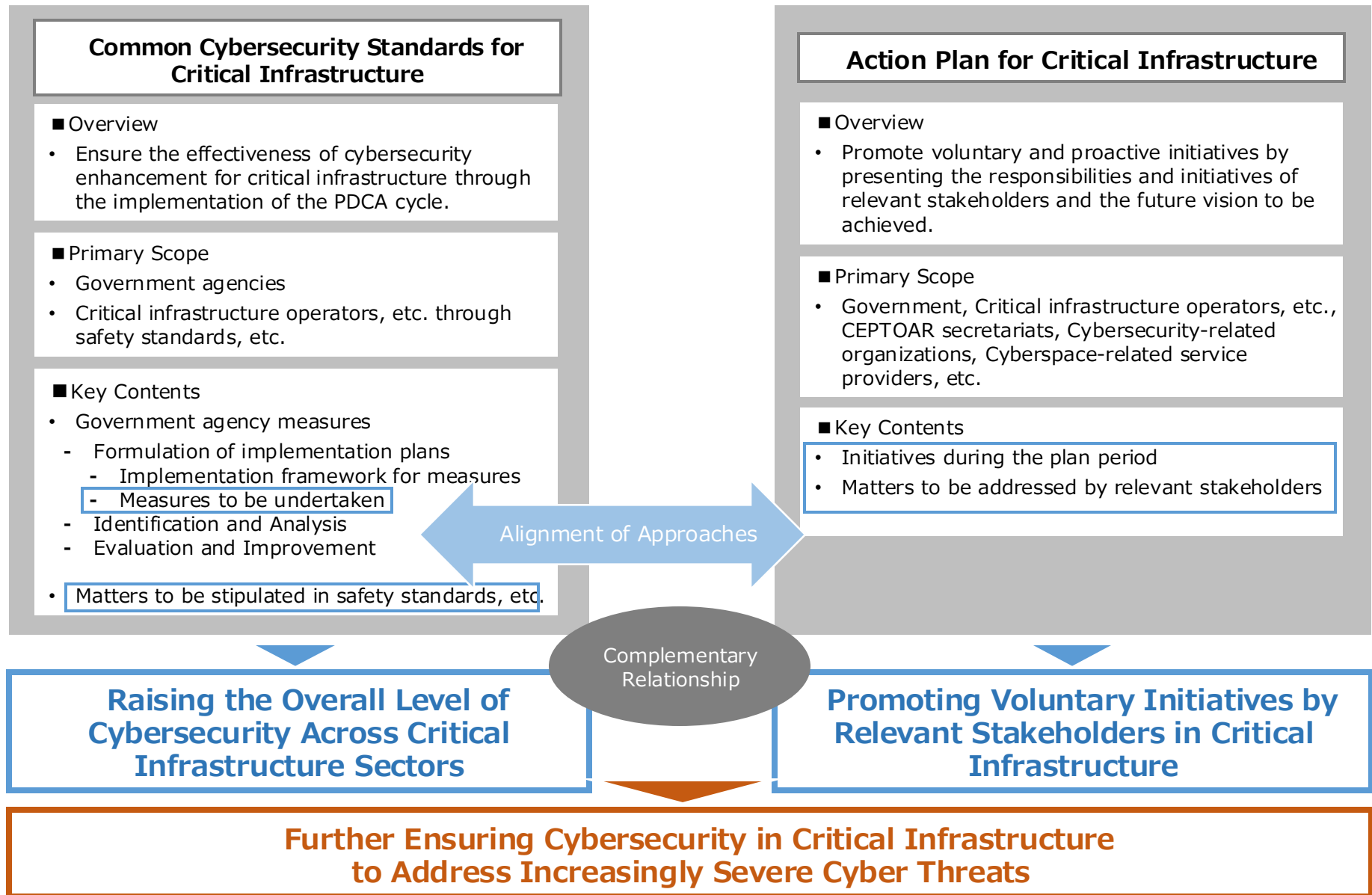
(As of July 2026)

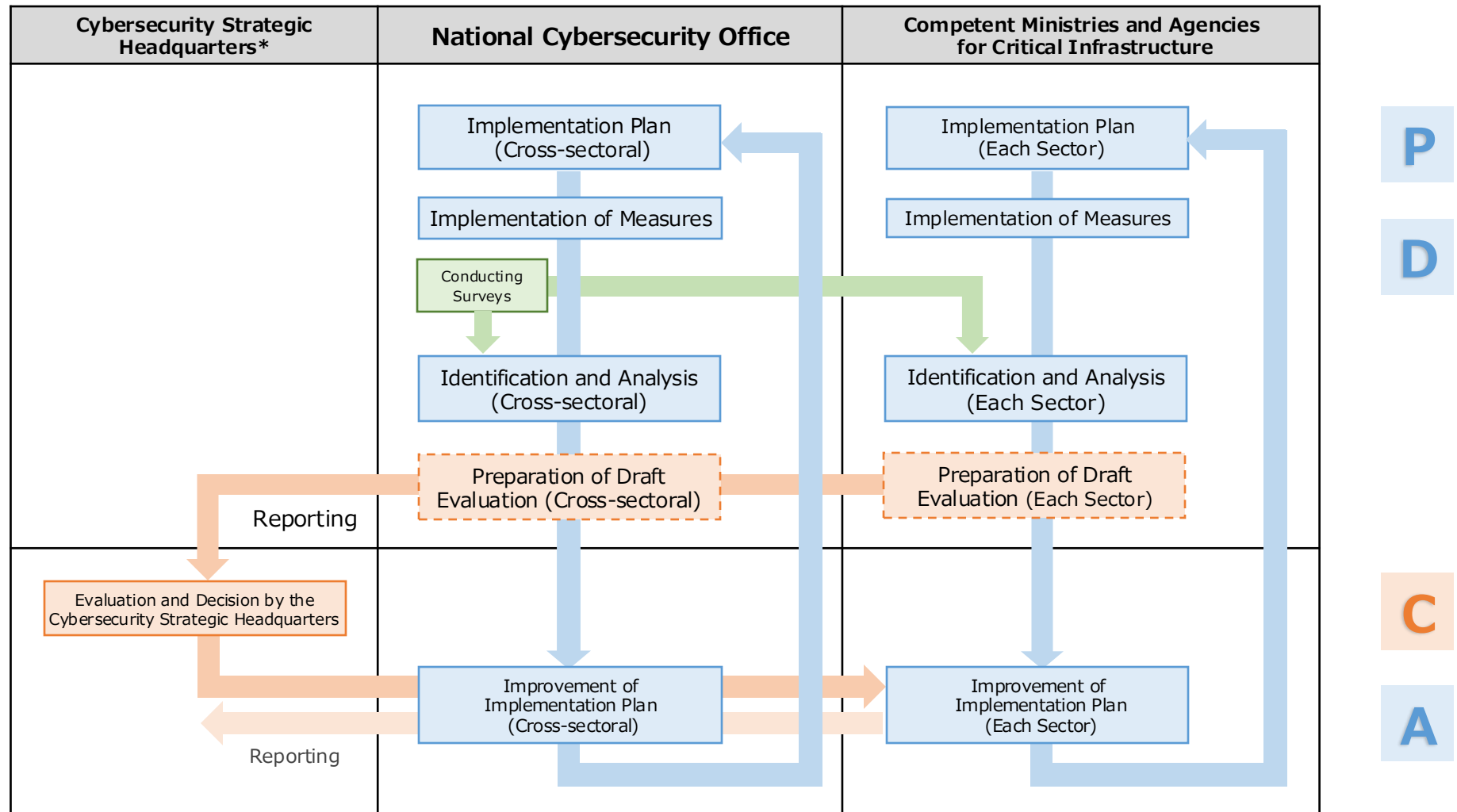
Overview of the Common Cybersecurity Standards for Critical Infrastructure₆

- Traditionally, the level of cybersecurity measures has varied across sectors and operators.
- To address increasingly severe cyber threats, such as state-sponsored attack campaigns, it is necessary to raise the baseline level of security measures across sectors and operators, and further enhance risk-based initiatives in each sector.



(Reference) Relationship Between the Common Cybersecurity Standards for Critical Infrastructure and the Action Plan





*Pursuant to the Basic Act on Cybersecurity, the opinions of the Critical Infrastructure Cybersecurity Measures Promotion Council are to be heard when compiling the results of evaluations of measures based on the Common Cybersecurity Standards for Critical Infrastructure.

- Part II describes the measures to be implemented by government agencies and how to ensure their effectiveness (PDCA cycle, identification of sectors and operators, etc.).
- Part III describes the items that should be stipulated in safety standards, etc. (ministerial ordinances, guidelines, etc.) in each sector as measures to be taken across sectors and operators by critical infrastructure operators, etc.

Common Cybersecurity Standards for Critical Infrastructure

Part I: General Provisions

- Purpose of the Common Cybersecurity Standards, etc.
- Scope of Application of the Common Cybersecurity Standards
- Improvement of Measures Based on the Common Cybersecurity Standards
- Structure of the Common Cybersecurity Standards, etc.
- Revision of the Common Cybersecurity Standards

Part II: Standards for Measures in Government Agencies

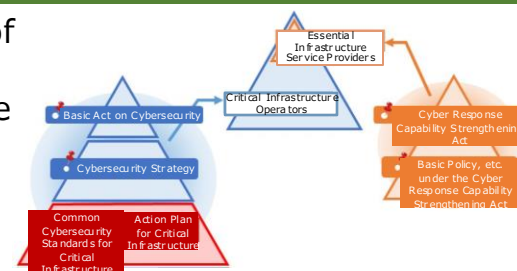
- Formulation of Implementation Plans
- Identification and Analysis
- Evaluation and Improvement

Part III: Items to Be Specified in Safety Standards, etc. ※ 1

- Basic Approach
- Organizational Governance
- Identification
- Protection
- Detection
- Response and Recovery
- Measures Based on Trends in Technologies and Threats, etc.

Scope of Application of the Common Cybersecurity Standards for Critical Infrastructure (Review of the Scope of Critical Infrastructure Protection)

- Ensure the thorough implementation of basic measures by related operators, including essential infrastructure service providers



Key Measures to Be Addressed through the Common Cybersecurity Standards for Critical Infrastructure (Examples)

- ① Updating the Assumption that “Closed Networks Are Secure”
- ② Addressing Supply Chain Risks
- ③ Enhancing Resilience to Reduce the Impact of Ransomware Attacks, etc.
- ④ Measures Based on Trends in Technologies and Threats, etc.
- ⑤ Strengthening Two-way Communication between the Public and Private Sectors

*1 For Part III, detailed items are described in the “Guidelines for Establishing Safety Standards, etc., for Cybersecurity of Critical Infrastructure,” to be referenced by competent ministries and agencies when formulating safety standards, etc.

*2 The specific contents of “Measures Based on Trends in Technologies and Threats, etc.” are described exclusively in the Guidelines for Establishing Safety Standards, etc.

- In principle, the scope of essential infrastructure will be included within the scope of critical infrastructure protection.
- This will strengthen cybersecurity for critical infrastructure by ensuring that relevant operators thoroughly implement basic measures to be taken across sectors and operators, including measures that serve as prerequisites for notifications and incident reporting by essential infrastructure service providers under the Cyber Response Capability Strengthening Act and Necessary Arrangement of Relevant Acts.
- To continuously improve cybersecurity levels for critical infrastructure, the critical infrastructure operators, etc. subject to the standards will be identified in the implementation plans.

