Приложение к исследованию

«Инфраструктура Интернета в контексте регулирования жизненно важных услуг и критических информационных инфраструктур: обзор международного и российского опыта»

Список основных документов, охватывающих регулирование Интернет-отрасли в контексте КИ, КИИ и жизненно важных услуг

08 августа 2016 г.

Оглавление

1. ОЭСР

OECD (2008), Recommendation of the Council on the Protection of Critical Information Infrastructures

(https://www.oecd.org/sti/40825404.pdf)

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The OECD is a unique forum where the governments of 30 democracies work together to address the economic, social and environmental challenges of globalisation. The OECD is also at the forefront of efforts to understand and to help governments respond to new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

The OECD member countries are: Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The Commission of the European Communities takes part in the work of the OECD.

Foreword

This Recommendation was developed by the OECD Committee for Information, Computer and Communication Policy (ICCP Committee), and its Working Party on Information Security and Privacy. The Recommendation was adopted by the OECD Council at its 1172nd Session on 30 April 2008.

OECD Recommendation of the Council on the Protection of Critical Information Infrastructures

THE COUNCIL

Having regard to Article 5 b) of the Convention on the Organisation for Economic Co-operation and Development of 14 December 1960;

Having regard to the Recommendation of the Council concerning Guidelines for the Security of Information Systems and Networks - Towards a Culture of Security [C(2002)131], hereinafter the "Security Guidelines";

Having regard to the Resolution 58/199 adopted by the General Assembly of the United Nations on the creation of a global culture of cybersecurity and the protection of critical information infrastructures;

Recognising that the functioning of our economies and societies increasingly relies on information systems and networks that are interconnected and interdependent, domestically and across borders; that a number of those systems and networks are of national critical

importance; and that their protection is a priority area for national policy and international cooperation;

Recognising that in order to improve the protection of domestic and cross- border critical information infrastructures, Member countries need to share their knowledge and experience in developing policies and practices and cooperate more closely between themselves as well as with non Member economies;

Recognising that the protection of critical information infrastructures requires coordination domestically and across borders with the private sector owners and operators of such infrastructures, hereinafter the "private sector";

On the proposal of the Committee for Information, Computer and Communication Policy:

AGREES that:

For the purposes of this Recommendation, critical information infrastructures, hereinafter "CII", should be understood as referring to those interconnected information systems and networks, the disruption or destruction of which would have a serious impact on the health, safety, security, or economic well-being of citizens, or on the effective functioning of government or the economy;

National CII are identified through a risk assessment process and typically include one or more of the following:

- Information components supporting critical infrastructures, and/or
- Information infrastructures supporting essential components of government business; and/or

- Information infrastructures essential to the national economy.

RECOMMENDS that:

Member countries introduce and maintain an effective framework to implement the OECD Security Guidelines in relation to the protection of CII, taking into account the specific policy and operational guidance set out herein;

PART I. Protection of critical information infrastructures at the domestic level

Member countries should:

Demonstrate government leadership and commitment to protect CII by:

- Adopting clear policy objectives at the highest level of government.

- Identifying government agencies and organisations with responsibility and authority to implement these policy objectives.

- Consulting with private sector owners and operators of CII to establish mutual cooperation for the implementation of these objectives.

- Ensuring transparency on the delegations of responsibility to government authorities and agencies to facilitate closer co-operation within the government and with the private sector.

- Systematically reviewing policy and legal frameworks and self-regulatory schemes which may apply to CII, including those addressing cross-border threats, to assess the need to enhance their implementation, to amend them or to develop new instruments.

- Taking steps, where appropriate, to enhance the security level of components of information system and networks that constitute CII.

Manage risks to CII by:

- Developing a national strategy that gains commitment from all those concerned, including the highest levels of government and the private sector.

- Taking into consideration interdependencies.

- Conducting a risk assessment based on the analysis of vulnerabilities and the threats to the CII, in order to protect economies and societies against the impacts of highest national concern.

- Developing, on the basis of the assessment, and periodically reviewing a national risk management process that sets out the detailed organisation, tools and monitoring mechanisms required to implement the risk management strategy at every level, including:

i. The appropriate organisational structure to provide guidelines and promote good security practices at the national level and to manage and monitor progress, as well as a complete set of processes to ensure
preparedness, including prevention, protection, response and recovery from natural and malicious threats.

ii. A system of measurement to evaluate and appraise measures in place (including exercises and tests as appropriate) and allow for feedback and continuous update.

- Developing an incident response capability, such as a computer security incident response team (CERT/CSIRTs), in charge of monitoring, warning, alerting and carrying out recovery measures for CII; and mechanisms to foster closer cooperation and communications among those involved in incident response.

Work in partnership with the private sector by:

- Establishing trusted public-private partnerships with a focus on risk management, incident response and recovery.

- Enabling mutual and regular exchange of information by establishing information sharing arrangements that acknowledge the sensitivity of certain information.

- Fostering innovation through public-private research and development projects focused on the improvement of the security of CII and as appropriate, sharing these innovations across borders.

PART II. Protecting critical information infrastructures across borders

Member countries should cooperate among themselves and with the private sector at the strategy, policy and operational levels to ensure the protection of CII against events and circumstances beyond the capacity of individual countries to address alone.

They should in particular proactively engage in bilateral and multilateral cooperation at regional and global levels with a view to:

- Share knowledge and experience with respect to the development of domestic policies and practices and to models for coordinating with private sector owners and operators of critical information infrastructures.

- Develop a common understanding of:

i. Risk management applicable to cross-border dependencies and inter-dependencies.

ii. Generic vulnerabilities, threats and impacts on the CII, to facilitate collective action to address those that are widespread, such as security flaws and malicious software, as well as to improve risk management strategies and policies.

- Make available information regarding the national agencies involved in the protection of CII, their roles and responsibilities, to facilitate identification of counterparts and improve the timeliness of cross border action.

- Acknowledge the value of participation in international or regional networks for watch, warning and incident response, to enable robust information sharing and coordination at the operational level, as well as to better manage crisis in case of an incident developing across borders.

- Support cross-border collaboration for, and information sharing on, public-private research and development for the protection of CII.

INVITES:

Member countries to disseminate this Recommendation throughout the public and private sectors, including governments, businesses and other international organisations to encourage all relevant participants to take the necessary steps for the protection of CII;

Non-Member economies to take account of this Recommendation and collaborate with Member countries in its implementation;

INSTRUCTS the OECD Committee for Information, Computer and Communication Policy to:

Promote the implementation of this Recommendation and review it every five years to foster international co-operation on issues relating to the protection of CII.

2. Аргентина

Ley 27.078 (Boletín Oficial Nº 33.034, 19/12/14) ARGENTINA DIGITAL

(http://www.enacom.gob.ar/ley-27-078_p2707)

Ley 27.078 (Boletín Oficial Nº 33.034, 19/12/14) ARGENTINA DIGITAL
Tecnologías de la Información y las Comunicaciones

[N. del CIT-ENACOM: El presente texto incluye las modificaciones efectuadas por el Decreto 267/2015; véase además dicho Decreto para mayor información sobre aspectos regulados por la presente]

Sancionada: Diciembre 16 de 2014
Promulgada: Diciembre 18 de 2014

El Senado y Cámara de Diputados de la Nación Argentina
reunidos en Congreso, etc. sancionan con fuerza de Ley:

LEY ARGENTINA DIGITAL

Título 1 Disposiciones Generales

Capítulo I Objeto

ARTÍCULO 1° — *Objeto*. Declárase de interés público el desarrollo de las Tecnologías de la In- formación y las Comunicaciones, las Telecomunicaciones, y sus recursos asociados, estable- ciendo y garantizando la completa neutralidad de las redes.

Su objeto es posibilitar el acceso de la totalidad de los habitantes de la República Argentina a los servicios de la información y las comunicaciones en condiciones sociales y geográficas equitati- vas, con los más altos parámetros de calidad.

Esta norma es de orden público y excluye cualquier tipo de regulación de los contenidos, cual- quiera fuere su medio de transmisión.

ARTÍCULO 2° — *Finalidad*. Las disposiciones de la presente ley tienen como finalidad garantizar el derecho humano a las comunicaciones y a las telecomunicaciones, reconocer a las Tecnolog- ías de la Información y las Comunicaciones (TIC) como un factor preponderante en la indepen- dencia tecnológica y productiva de nuestra Nación, promover el rol del Estado como planificador, incentivando la función social que dichas tecnologías poseen, como así también la competencia y la generación de empleo mediante el establecimiento de pautas claras y transparentes que favorezcan el desarrollo sustentable del sector, procurando la accesibilidad y asequibilidad de las tecnologías de la información y las comunicaciones para el pueblo. Asimismo, se busca establecer con claridad la distinción entre los mercados de generación de contenidos y de transporte y distribución de manera que la influencia en uno de esos mercados no genere prácticas que impliquen distorsiones en el otro.

En la ejecución de la presente ley se garantizará el desarrollo de las economías regionales, pro- curando el fortalecimiento de los actores locales existentes, tales como cooperativas, entidades sin fines de lucro y pymes, propendiendo a la generación de nuevos actores que en forma indivi- dual o colectiva garanticen la prestación de los Servicios de TIC.

ARTÍCULO 3° — *Ámbito de aplicación*. La presente ley es de aplicación en todo el territorio de la Nación Argentina y en los lugares sometidos a su jurisdicción.

ARTÍCULO 4° — *Jurisdicción federal y competencia contencioso administrativa*. Las actividades reguladas por la presente estarán sujetas a la jurisdicción federal y cualquier incidencia que de modo directo o indirecto pudiera surgir o derivar de la aplicación de la presente será competen- cia del fuero Contencioso Administrativo Federal, con excepción de las relaciones de consumo.

ARTÍCULO 5° — *Inviolabilidad de las comunicaciones.* La correspondencia, entendida como toda comunicación que se efectúe por medio de Tecnologías de la Información y las Comunica- ciones (TIC), entre las que se incluyen los tradicionales correos postales, el correo electrónico o cualquier otro mecanismo que induzca al usuario a presumir la privacidad del mismo y de los datos de tráfico asociados a ellos, realizadas a través de las redes y servicios de telecomunica- ciones, es inviolable. Su interceptación, así como su posterior registro y análisis, sólo procederá a requerimiento de juez competente.

Capítulo II Definiciones

ARTÍCULO 6° **[texto vigente a partir del Dec. 267/2015]**.- Definiciones generales. En lo que res- pecta al régimen de las Tecnologías de la Información y las Comunicaciones y de las Teleco- municaciones (TIC), se aplicarán las siguientes definiciones:

a) Radiodifusión por suscripción: Toda forma de comunicación primordialmente unidireccional destinada a la transmisión de señales para ser recibidas por público determinable, mediante la utilización del espectro radioeléctrico o mediante vínculo físico indistintamente. Incluye el servi- cio de radiodifusión ofrecido por un prestador de servicios TIC que utilice la tecnología de transmisión de contenidos audiovisuales basados en el protocolo IP (IPTV), para el acceso de los programas en vivo y/o televisión lineal.

b) Radiodifusión por suscripción mediante vínculo físico: Toda forma de radiocomunicación primordialmente unidireccional destinada a la transmisión de señales para ser recibidas por públicos determinables, mediante la utilización de medios físicos.

c) Radiodifusión por suscripción mediante vínculo radioeléctrico: Toda forma de comunicación primordialmente unidireccional destinada a la transmisión de señales para ser recibidas por público determinable, mediante la utilización del espectro radioeléctrico.

d)

e) Recursos asociados: son las infraestructuras físicas, los sistemas, los dispositivos, los servi- cios asociados u otros recursos o elementos asociados con una red de telecomunicaciones o con un Servicio de TIC que permitan o apoyen la prestación de servicios a través de dicha red o servicio, o tengan potencial para ello. Incluirán, entre otros, edificios o entradas de edificios, el cableado de edificios, antenas, torres y otras

construcciones de soporte, conductos, mástiles, bocas de acceso y distribuidores.

f) Servicio Básico Telefónico (SBT): consiste en la provisión del servicio de telefonía nacional e internacional de voz, a través de las redes locales, independientemente de la tecnología utiliza- da para su transmisión, siempre que cumpla con la finalidad de permitir a sus usuarios comuni- carse entre sí.

g) Servicio de video a pedido o a demanda: servicio ofrecido por un prestador de servicios de TIC para el acceso a programas en el momento elegido y a petición propia, sobre la base de un catálogo.

h) Servicios de Tecnologías de la Información y las Comunicaciones (Servicios de TIC): son aquellos que tienen por objeto transportar y distribuir señales o datos, como voz, texto, video e imágenes, facilitados o solicitados por los terceros usuarios, a través de redes de telecomuni- caciones. Cada servicio estará sujeto a su marco regulatorio específico.

i) Servicio de Telecomunicación: es el servicio de transmisión, emisión o recepción de escritos, signos, señales, imágenes, sonidos o información de cualquier naturaleza, por hilo, radioelec- tricidad, medios ópticos u otros sistemas electromagnéticos, a través de redes de telecomuni- caciones.

j) Tecnologías de la información y las comunicaciones (TIC): es el conjunto de recursos, herra- mientas, equipos, programas informáticos, aplicaciones, redes y medios que permitan la compi- lación, procesamiento, almacenamiento y transmisión de información, como por ejemplo voz, datos, texto, video e imágenes, entre otros.

k) Telecomunicación: es toda transmisión, emisión o recepción de signos, señales, escritos, imágenes, sonidos o información de cualquier naturaleza, por hilo, radioelectricidad, medios ópticos u otros sistemas electromagnéticos".

ARTÍCULO 7° — *Definiciones particulares*. En la relación entre los licenciatarios o prestadores de Servicios de TIC se aplicarán las siguientes definiciones:

a) *Acceso*: es la puesta a disposición de parte de un prestador a otro de elementos de red, re- cursos asociados o servicios con fines de prestación de Servicios de TIC, incluso cuando se utili- cen para el suministro de servicios de contenidos audiovisuales.

b) *Arquitectura abierta*: es el conjunto de características técnicas de las redes de telecomunica- ciones que les permite interconectarse entre sí a nivel físico o virtual, lógico y funcional, de tal manera que exista interoperabilidad entre ellas.

c) *Facilidades esenciales*: son los elementos de red o servicios que se proporcionan por un solo licenciatario o prestador o un reducido número de ellos cuya reproducción no es viable desde un punto de vista técnico, legal o económico y son insumos indispensables para la prestación de los servicios previstos en esta ley. En los casos no previstos en la presente, la Autoridad de Aplica- ción determinará la existencia y regulación al acceso a las facilidades esenciales en términos de lo dispuesto por la ley 25.156 o la que en el futuro la reemplace.

d) *Interconexión*: es la conexión física y lógica de las redes de telecomunicaciones de manera tal que los usuarios de un licenciatario puedan comunicarse con los usuarios de

otro licenciatario, así como también acceder a los servicios brindados por otro licenciatario. Los servicios podrán ser facilitados por las partes interesadas o por terceros que tengan acceso a la red. La interco- nexión constituye un tipo particular de acceso entre prestadores de Servicios de TIC.

e) *Red de telecomunicaciones*: son los sistemas de transmisión y, cuando proceda, los equipos de conmutación o encaminamiento y demás recursos, incluidos los elementos que no son acti- vos, que permitan el transporte de señales mediante cables, ondas hertzianas, medios ópticos u otros medios electromagnéticos, con inclusión de las redes de satélites, redes terrestres fijas (de conmutación de circuitos y de paquetes u otros) y móviles, sistemas de tendido eléctrico, en la medida en que se utilicen para la transmisión de señales, redes utilizadas para la radiodifusión sonora y televisiva y redes de televisión por cable, con independencia del tipo de información transportada.

f) *Red local*: es la infraestructura de red de telecomunicaciones, incluyendo el software y el hardware necesarios para llevar a cabo la conectividad desde el punto de conexión terminal de la red ubicado en el domicilio del usuario a la central telefónica o instalación equivalente, cir- cunscripta a un área geográfica determinada.

g) *Usuario de Servicios de TIC*: es la persona física o jurídica que utiliza el servicio para sí. No incluye la prestación, reventa o arriendo de las redes o servicios disponibles para el público.

h) *Poder significativo de mercado*: es la posición de fuerza económica que le permite a uno o más prestadores que su comportamiento sea, en una medida apreciable, independiente de sus competidores. Esta fuerza económica puede estar fundada en la cuota de participación en el o los mercados de referencia, en la propiedad de facilidades esenciales, en la capacidad de influir en la formación de precios o en la viabilidad de sus competidores; incluyendo toda situación que permita o facilite el ejercicio de prácticas anticompetitivas por parte de uno o más prestadores a partir, por ejemplo, de su grado de integración vertical u horizontal. Las obligaciones específicas impuestas al prestador con poder significativo de mercado se extinguirán en sus efectos por re- solución de la Autoridad de Aplicación una vez que existan condiciones de competencia efectiva en el o los mercados de referencia. La Autoridad de Aplicación está facultada para declarar en cualquier momento prestadores con poder significativo de mercado en los servicios de aplicación de la presente ley de acuerdo al procedimiento que establezca la reglamentación.

Título II Licencias

ARTÍCULO 8° — *Régimen*. La prestación de los Servicios de TIC se realizará en régimen de competencia.
Para la prestación de Servicios de TIC se requerirá la previa obtención de la licencia habilitante. El licenciatario de Servicios de TIC deberá proceder a la registración de cada servicio en las condiciones que determine la Autoridad de Aplicación.

ARTÍCULO 9° — *Principios*. Las licencias se otorgarán a pedido y en la forma reglada, habilitan- do a la prestación de los servicios previstos en esta ley en todo el territorio de la Nación Argenti- na, sean fijos o móviles, alámbricos o inalámbricos, nacionales o internacionales, con o sin infra- estructura propia.

Los licenciatarios de los servicios previstos en esta ley podrán brindar servicios de comunicación audiovisual, con excepción de aquellos brindados a través de vínculo satelital, debiendo tramitar la licencia correspondiente ante la autoridad competente. Asimismo, los licenciatarios de servi- cios de comunicación audiovisual podrán brindar Servicios de TIC, debiendo tramitar la licencia correspondiente ante la Autoridad de Aplicación de la presente ley.

Quedan exceptuados los licenciatarios de servicios públicos relacionados con el ámbito de apli- cación de la presente ley, de las disposiciones contenidas en los artículos 24 inciso i) y 25 inciso
d) de la ley 26.522, sean éstas personas físicas o jurídicas respectivamente.

ARTÍCULO 10 **[texto vigente a partir del Dec. 267/2015]**.- Incorpórase como servicio que podrán registrar los licenciatarios de TIC, al servicio de Radiodifusión por suscripción, mediante vínculo físico y/o mediante vínculo radioeléctrico. El servicio de Radiodifusión por suscripción se regirá por los requisitos que establecen los artículos siguientes de la presente ley y los demás que establezca la reglamentación, no resultándole aplicables las disposiciones de la Ley N° 26.522. Se encuentra excluida de los servicios de TIC la televisión por suscripción satelital que se con- tinuara rigiendo por la Ley N° 26.522.

Las licencias de Radiodifusión por suscripción mediante vínculo físico y/o mediante vínculo radioeléctrico otorgadas por el ex COMITÉ FEDERAL DE RADIODIFUSIÓN y/o por la AUTORIDAD FEDERAL DE SERVICIOS DE COMUNICACIÓN AUDIOVISUAL con anterioridad a la entrada en vigencia de la modificación del presente artículo serán consideradas, a todos los efectos, Licencia Única Argentina Digital con registro de servicio de Radiodifusión por Sus- cripción mediante vínculo físico o mediante vínculo radioeléctrico, en los términos de los artícu- los 8° y 9° de esta ley, debiendo respetar los procedimientos previstos para la prestación de nuevos servicios salvo que ya los tuvieren registrados.

El plazo de otorgamiento del uso de las frecuencias del espectro radioeléctrico de los titulares de licencias de Radiodifusión por Suscripción conferidas bajo las Leyes Nros. 22.285 y 26.522 será el de su título original, o de DIEZ (10) años contados a partir del 1° de enero de 2016, siempre el que sea mayor para aquellos que tuvieren a dicha fecha una licencia vigente.

ARTÍCULO 11. — *Condiciones de prestación*. El otorgamiento de la licencia para la prestación de los servicios previstos en esta ley es independiente de la tecnología o medios utilizados para ofrecerlos y de la existencia y asignación de los medios requeridos para la prestación del servi- cio.

ARTÍCULO 12. — *Requisitos*. La Autoridad de Aplicación otorgará la licencia una vez que el soli- citante haya dado cumplimiento a los requisitos que establezca la reglamentación. Si para la prestación del Servicio de TIC se requiere el uso de frecuencias del espectro radio- eléctrico, el licenciatario deberá tramitar, de conformidad con lo dispuesto en la normativa es- pecífica en la materia, el otorgamiento de la correspondiente autorización o permiso de uso de frecuencias del espectro radioeléctrico.

ARTÍCULO 13 **[texto vigente a partir del Dec. 267/2015]**.- Los licenciatarios deberán obtener au- torización del ENACOM, para efectuar cualquier modificación de las participaciones accionarias o cuotas sociales en las sociedades titulares, que impliquen la pérdida del control social en los términos del artículo 33 de la LEY GENERAL DE

SOCIEDADES Nº 19.550, T.O. 1984 y sus modificatorias, sin perjuicio del cumplimiento de lo dispuesto en la Ley Nº 25.156.

Las transferencias de licencias y de participaciones accionarias o cuotas sociales sobre sociedades licenciatarias, se considerarán efectuadas ad referéndum de la aprobación del ENACOM, y deberán ser comunicadas dentro de los TREINTA (30) días posteriores a su per- feccionamiento. Si el ENACOM no hubiera rechazado expresamente la transferencia dentro de los NOVENTA (90) días de comunicada, la misma se entenderá aprobada tácitamente, y quien corresponda podrá solicitar el registro a su nombre. En caso de existir observaciones, el plazo referido se contará desde que se hubieran considerado cumplidas las mismas, con los mismos efectos.

La ejecución del contrato de transferencia sin la correspondiente aprobación, expresa o tácita, será sancionada con la caducidad de pleno derecho de la licencia adjudicada, previa intimación del ENACOM.

ARTÍCULO 14. — *Caducidad o extinción de la licenci*a. La Autoridad de Aplicación podrá decla- rar la caducidad de la licencia o registro respectivo, conforme lo dispuesto por la presente ley, los decretos, reglamentos y demás normativa vigente en la materia, contemplando el procedimiento establecido por aquélla.

Serán causales de caducidad:

a) La falta de prestación del o de los servicios registrados conforme la normativa vigente.

b) La falta de inicio de la prestación del o de los servicios registrados dentro del plazo que esta- blezca la normativa vigente y de conformidad con la normativa que al efecto dicte la Autoridad de Aplicación.

c) La falta reiterada de pago de tasas, derechos, cánones y el aporte al Servicio Universal, de conformidad con la reglamentación que al efecto dicte la Autoridad de Aplicación.

d) La materialización de actos sin la autorización del artículo 13 de la presente.

e) La quiebra, disolución o liquidación del licenciatario.

Título III

Servicios de TIC y establecimiento y explotación de redes de telecomunicaciones

Capítulo I Principios generals

ARTÍCULO 15 **[derogado por Dec.267/2015]**.

ARTÍCULO 16. — *Homologación y certificación*. *Principio*. Con el objeto de garantizar la integri- dad y calidad de las redes de telecomunicaciones y del espectro radioeléctrico, así

como tam- bién la seguridad de las personas, usuarios y licenciatarios, los equipos de telecomunicaciones que sean comercializados estarán sujetos a homologación y certificación. La Autoridad de Apli- cación dictará el reglamento respectivo.

Capítulo II Mecanismos de coordinación

ARTÍCULO 17. — *Mecanismos de coordinación para el despliegue de redes de telecomunica- cione*s. Las autoridades nacionales, provinciales, de la Ciudad Autónoma de Buenos Aires y mu- nicipales, coordinarán las acciones necesarias para lograr el despliegue de las redes de teleco- municaciones utilizadas en los Servicios de TIC. La Autoridad de Aplicación invitará a las provin- cias, a la Ciudad Autónoma de Buenos Aires y a los municipios a suscribir los respectivos con- venios de cooperación.

Título IV Desarrollo de las TIC

Capítulo I Servicio Universal

ARTÍCULO 18. — *Definición*. El Estado nacional garantiza el Servicio Universal, entendido como el conjunto de Servicios de TIC que deben prestarse a todos los usuarios, asegurando su acceso en condiciones de calidad, asequibilidad y a precios justos y razonables, con independencia de su localización geográfica.

ARTÍCULO 19. — *Finalidad*. El Servicio Universal es un concepto dinámico cuya finalidad es posibilitar el acceso de todos los habitantes de nuestro país, independientemente de su domici- lio, ingreso o capacidades, a los Servicios de TIC prestados en condiciones de calidad y a un precio justo y razonable.

ARTÍCULO 20. — *Alcance y régimen*. Corresponde al Poder Ejecutivo nacional, a través de la Autoridad de Aplicación, definir la política pública a implementar para alcanzar el objetivo del Servicio Universal. Sin perjuicio de ello, el Servicio Universal se regirá por los principios, proce- dimientos y disposiciones de la presente ley y, en particular, por las resoluciones que a tal efecto dicte la Autoridad de Aplicación.

Capítulo II

Fondo Fiduciario del Servicio Universal

ARTÍCULO 21. — *Creación y financiamiento*. Créase el Fondo Fiduciario del Servicio Universal. Los aportes de inversión correspondientes a los programas del Servicio Universal serán adminis- trados a través de dicho fondo. El patrimonio del Fondo Fiduciario del Servicio Universal será del Estado nacional. La Autoridad de Aplicación dictará el reglamento de administración del Fondo y las reglas para su control y auditoría respecto de los costos de administración, asegurando que tanto la misma como la ejecución del Fondo se encuentren a cargo del Estado nacional.

ARTÍCULO 22. — *Aportes de inversión*. Los licenciatarios de Servicios de TIC tendrán la obliga- ción de realizar aportes de inversión al Fondo Fiduciario del Servicio Universal equivalente al uno por ciento (1%) de los ingresos totales devengados por la prestación de los Servicios de TIC incluidos en el ámbito de aplicación de esta ley, netos de los impuestos

y tasas que los graven o, en caso de otorgarse exenciones, cumplir con las obligaciones en ellas establecidas. El aporte de inversión no podrá ser trasladado a los usuarios bajo ningún concepto. El Fondo Fiduciario del Servicio Universal podrá integrarse también con donaciones o legados.

ARTÍCULO 23. — *Exención de aporte*. La Autoridad de Aplicación podrá disponer, una vez al- canzados los objetivos del Servicio Universal, la exención total o parcial, permanente o temporal, de la obligación de realizar los aportes de inversión dispuestos en el artículo anterior.

ARTÍCULO 24. — *Categorías del Servicio Universal*. La Autoridad de Aplicación diseñará los distintos programas para el cumplimiento de las obligaciones y el acceso a los derechos previs- tos respecto del Servicio Universal, pudiendo establecer categorías a tal efecto.

ARTÍCULO 25. — *Aplicación de fondos*. Los fondos del Servicio Universal se aplicarán por me- dio de programas específicos. La Autoridad de Aplicación definirá su contenido y los mecanis- mos de adjudicación correspondientes. La Autoridad de Aplicación podrá encomendar la ejecu- ción de estos planes directamente a las entidades incluidas en el artículo 8°, inciso b), de la ley 24.156, o, cumpliendo con los mecanismos de selección que correspondan, respetando princi- pios de publicidad y concurrencia, a otras entidades.

Los programas del Servicio Universal deben entenderse como obligaciones sujetas a revisión periódica, por lo que los servicios incluidos y los programas que se elaboren serán revisados, al menos cada dos (2) años, en función de las necesidades y requerimientos sociales, la demanda existente, la evolución tecnológica y los fines dispuestos por el Estado nacional de conformidad con el diseño de la política de las Tecnologías de la Información y las Comunicaciones (TIC).

Título V

Recursos esenciales de las TIC Capítulo I

Espectro radioeléctrico

ARTÍCULO 26. — *Características*. El espectro radioeléctrico es un recurso intangible, finito y de dominio público, cuya administración, gestión y control es responsabilidad indelegable del Esta- do nacional.

ARTÍCULO 27. — *Administración, gestión y control*. Corresponde a la Autoridad de Aplicación que se designe la administración, gestión y control del espectro radioeléctrico, de conformidad con lo que establece esta ley, la reglamentación que en su consecuencia se dicte, las normas internacionales y aquellas dictadas por las conferencias mundiales y regionales en la materia a las que la República Argentina adhiera.

ARTÍCULO 28. — *Autorizaciones y permiso*s. Las autorizaciones y los permisos de uso de fre- cuencias del espectro radioeléctrico se otorgarán con carácter precario, por lo que la Autoridad de Aplicación podrá sustituirlos, modificarlos o cancelarlos, total o parcialmente, sin que ello dé lugar a derecho de indemnización alguna a favor del autorizado o administrado.

Las autorizaciones y permisos de uso de frecuencia del espectro radioeléctrico asignados por licitación o concurso público, con carácter oneroso, se regirán por los términos fijados al momen- to de dicha licitación o concurso, de conformidad con el marco del régimen de contrataciones de la administración nacional, salvo fundadas razones de interés público debidamente acreditadas.

Para todos los casos mencionados, la Autoridad de Aplicación fijará el plazo máximo de otorga- miento de cada autorización o permiso.

ARTÍCULO 29. — *Cesión y arrendamiento*. Las autorizaciones y permisos de uso de frecuencia del espectro radioeléctrico y las autorizaciones y habilitaciones otorgadas para instalar y operar una estación, medios o sistemas radioeléctricos, no podrán ser transferidas, arrendadas ni cedi- das total o parcialmente ni cambiarles su destino, sin la aprobación previa de la Autoridad de Aplicación, conforme a la normativa vigente.

ARTÍCULO 30. — *Migración de bandas*. La Autoridad de Aplicación podrá requerir a los titulares de autorizaciones y permisos de uso de frecuencias la migración de sus sistemas como conse- cuencia de cambios en la atribución de bandas de frecuencias. La migración deberá cumplirse en los plazos que fije la Autoridad de Aplicación. Los autorizados o permisionarios no tienen de- recho a indemnización alguna.

ARTÍCULO 31. — *Asignación directa*. La Autoridad de Aplicación podrá asignar en forma directa frecuencias a organismos nacionales, entidades estatales y entidades con participación mayori- taria del Estado nacional.

ARTÍCULO 32. — *Autorización*. Los licenciatarios de Servicios de TIC deberán contar con auto- rización previa para la instalación, modificación y operación de estaciones, medios o sistemas de radiocomunicación.

Capítulo II Uso satelital

ARTÍCULO 33 **[texto vigente a partir del Dec. 267/2015]**.- Administración, Gestión y Control. Co- rresponde al Estado Nacional, a través del MINISTERIO DE COMUNICACIONES, la adminis- tración, gestión y control de los recursos órbita-espectro correspondientes a redes satelitales, de conformidad con los tratados internacionales suscriptos y ratificados por el Estado Argenti- no.

Este recurso podrá ser explotado por entidades de carácter público o privado siempre que me- die autorización otorgada al efecto y de conformidad con las disposiciones aplicables en la ma- teria.

ARTÍCULO 34 **[texto vigente a partir del Dec. 267/2015].** Autorización. La prestación de facilida- des satelitales requerirá la correspondiente autorización para la operación en la Argentina, con- forme a la reglamentación que el MINISTERIO DE COMUNICACIONES dicte a tal efecto. Por el contrario, la prestación de cualquier Servicio de TIC por satélite estará sometida al régimen general de prestación de Servicios de TIC establecido en la presente ley.

ARTÍCULO 35 **[texto vigente a partir del Dec. 267/2015]**. Prioridad de uso. Para la

prestación de las facilidades satelitales se dará prioridad al uso de satélites argentinos, entendiéndose por tales a los que utilicen un recurso órbita-espectro a nombre de la Nación Argentina, a la utiliza- ción de satélites construidos en la Nación Argentina o a las empresas operadoras de satélites que fueran propiedad del Estado nacional o en las que éste tuviera participación accionaria mayoritaria.

La prioridad señalada precedentemente tendrá efecto sólo si las condiciones técnicas y econó- micas propuestas se ajustan a un mercado de competencia, lo cual será determinado por el MINISTERIO DE COMUNICACIONES.

Capítulo III Planes fundamentals

ARTÍCULO 36. — *Dictado de los planes*. La Autoridad de Aplicación debe aprobar, gestionar y controlar los planes nacionales de numeración, señalización, portabilidad numérica y otros pla- nes fundamentales, y tiene la facultad de elaborarlos o modificarlos.

ARTÍCULO 37. — *Atributos*. Los atributos de los planes fundamentales tienen carácter instru- mental y su otorgamiento no confiere derechos e intereses a los licenciatarios de Servicios de TIC, motivo por el cual su modificación o supresión no genera derecho a indemnización alguna. Capítulo IV Acceso e interconexión

ARTÍCULO 38. — *Alcance*. Este capítulo y su reglamentación serán de aplicación a los supues- tos de uso y acceso e interconexión entre los licenciatarios de Servicios de TIC.

ARTÍCULO 39. — *Obligación de acceso e interconexión*. Los licenciatarios de Servicios de TIC tendrán el derecho y, cuando se solicite por otros licenciatarios de TIC, la obligación de suminis- trar el acceso y la interconexión mutua.

ARTÍCULO 40. — *Régimen general*. Los licenciatarios de Servicios de TIC están obligados a interconectarse en condiciones no discriminatorias, transparentes y basadas en criterios objeti- vos, conforme las disposiciones dictadas por la Autoridad de Aplicación, las que fomentarán la competencia y se orientarán a la progresiva reducción de asimetrías entre licenciatarios.

Los términos y condiciones para acceso o interconexión que un licenciatario de Servicios de TIC ofrezca a otro con motivo de un acuerdo o de una resolución de la Autoridad de Aplicación, de- berán ser garantizados a cualquier otro que lo solicite.

Los licenciatarios ajenos a la relación contractual podrán realizar observaciones al acuerdo sus- cripto conforme lo disponga la reglamentación.

ARTÍCULO 41. — *Condiciones particulares*. La Autoridad de Aplicación podrá determinar condi- ciones particulares de acceso e interconexión con las redes que fueran propiedad del Estado nacional o de sociedades con participación estatal mayoritaria.

ARTÍCULO 42. — *Registro y publicación*. Los acuerdos entre licenciatarios de Servicios de TIC deberán registrarse ante la Autoridad de Aplicación y publicarse de acuerdo a la reglamentación vigente.

ARTÍCULO 43. — *Ofertas de referencia*. Las ofertas de referencia deberán someterse a la

auto- rización y la publicación por parte de la Autoridad de Aplicación de acuerdo a las disposiciones dictadas por ésta.

En los casos comprendidos en el artículo 10 de la presente ley, la oferta de referencia deberá garantizar que el tratamiento dado a sus unidades de negocio no distorsiona la competencia en el mercado de referencia.

ARTÍCULO 44. — *Diseño de arquitectura abierta*. Los licenciatarios de Servicios de TIC deberán adoptar diseños de arquitectura abierta de red para garantizar la interconexión y la interoperabi- lidad de sus redes.

ARTÍCULO 45. — *Desagregación de red local*. Se dispone la desagregación de la red local de los licenciatarios de Servicios de TIC. La Autoridad de Aplicación establecerá a tal fin las condi- ciones diferenciadas fundadas en cuestiones técnicas, económicas, de oportunidad, mérito y conveniencia, atendiendo a la preservación del interés público y promoviendo la competencia.

ARTÍCULO 46. — *Obligaciones específicas*. Aquellos licenciatarios de Servicios de TIC con po- der significativo de mercado deberán cumplir con las obligaciones específicas que sean dispues- tas por la Autoridad de Aplicación, las que garantizarán por medio de medidas regulatorias asimétricas el desarrollo de los mercados regionales, la participación de los licenciatarios locales y la continuidad en la prestación de los servicios de TIC.

ARTÍCULO 47. — *Competencias*. Son competencias de la Autoridad de Aplicación en materia de acceso e interconexión:

a) Disponer las condiciones jurídicas, técnicas y económicas a las que deberán ceñirse los acuerdos.

b) Llevar registro de los acuerdos celebrados y efectuar el análisis previo a la autorización de una oferta de referencia.

c) Intervenir, de oficio o a petición de cualquiera de las partes interesadas, instando a efectuar las modificaciones al acuerdo suscripto que estime corresponder.

d) Establecer obligaciones y condiciones específicas para aquellos licenciatarios, con poder sig- nificativo de mercado y cualquier otro que considere justificadamente necesario; dichas obliga- ciones se mantendrán en vigor durante el tiempo estrictamente imprescindible y podrán consistir en:

i. El suministro de información contable, económica y financiera, especificaciones técnicas, ca- racterísticas de las redes y condiciones de suministro y utilización, incluidas, en su caso, las condiciones que pudieran limitar el acceso o la utilización de servicios o aplicaciones, así como los precios y tarifas.

ii. La elaboración, presentación y publicación de una oferta de referencia bajo las condiciones establecidas reglamentariamente.

iii. La separación de cuentas, en el formato y con la metodología que, en su caso,

se especifi- quen.

iv. La separación funcional.

v. Brindar acceso a elementos o a recursos específicos de las redes y a su utilización, así como a recursos y servicios asociados.

vi. Control de precios y tarifas, tales como su fijación, su orientación en función de los costos o la determinación de otro tipo de mecanismo de compensación.

vii. Deber de notificación para su aprobación previa, ante la necesidad de efectuar modificacio- nes en la red que afecten el funcionamiento de los equipos de los usuarios o de las redes con las que esté interconectada.

viii. Otro tipo de obligaciones específicas relativas al acceso o a la interconexión que no se limi- ten a las materias enumeradas anteriormente y que estén debidamente justificadas.

Título VI

Precios, tarifas y gravámenes

ARTÍCULO 48. — *Regla*. Los licenciatarios de Servicios de TIC fijarán sus precios, los que de- berán ser justos y razonables, cubrir los costos de la explotación y tender a la prestación eficien- te y a un margen razonable de operación. **[El párrafo siguiente fue derogado por el Dec. 267/2015]**

ARTÍCULO 49. — *Tasa de control, fiscalización y verificación*. Establécese para los licenciatarios de Servicios de TIC una tasa en concepto de control, fiscalización y verificación, equivalente a cero coma cincuenta por ciento (0,50%) de los ingresos totales devengados por la prestación de los Servicios de TIC, netos de los impuestos y tasas que los graven.

La Autoridad de Aplicación establecerá el tiempo, forma y procedimiento relativo al cobro de la tasa fijada en el primer párrafo de este artículo, con el propósito de permitir la financiación de las erogaciones que hacen a su funcionamiento.

ARTÍCULO 50. — *Derechos y aranceles radioeléctricos*. Los licenciatarios de Servicios de TIC en general y de telecomunicaciones en particular deberán abonar los derechos y aranceles ra- dioeléctricos para cada una de las estaciones, sistemas y servicios radioeléctricos que operan en todo el territorio de la Nación, cuya unidad de medida será la denominada Unidad de Tasación Radioeléctrica (UTR). La clasificación, valor, actualización, periodicidad de pago, penalidades y exenciones serán determinados por la Autoridad de Aplicación.

ARTÍCULO 51. — *Aranceles administrativos*. La Autoridad de Aplicación tendrá la facultad de fijar aranceles administrativos.

ARTÍCULO 52. — *Tasas y gravámenes específicos*. Las tasas y gravámenes para establecer sistemas y estaciones de telecomunicaciones no abiertos a la correspondencia pública se de- terminarán de acuerdo con las características de los mismos, la importancia de

sus instalaciones y la evaluación del tráfico previsible, conforme a lo previsto en la reglamentación.

ARTÍCULO 53. — *Exenciones*. Podrán establecerse a título precario exenciones o reducciones de tasas, tarifas y gravámenes de Tecnologías de la Información y las Comunicaciones (TIC) en general y telecomunicaciones en particular, cuando la índole de determinadas actividades lo jus- tifique.

Título VII

Consideraciones generales sobre los Servicios de TIC

ARTÍCULO 54. — *Servicio Público Telefónico*. El Servicio Básico Telefónico mantiene su condi- ción de servicio público.

ARTÍCULO 55. — *Objeto y alcance*. El Servicio de TIC comprende la confluencia de las redes tanto fijas como móviles que, mediante diversas funcionalidades, proporciona a los usuarios la capacidad de recibir y transmitir información de voz, audio, imágenes fijas o en movimiento y datos en general.

A los efectos de resguardar la funcionalidad del Servicio de TIC, éste deberá ser brindado en todo el territorio nacional considerado a tales efectos como una única área de explotación y pres- tación.

El Servicio Básico Telefónico, sin perjuicio de su particularidad normativa, reviste especial consi- deración dentro del marco de la convergencia tecnológica. Es por ello que la efectiva prestación del servicio debe ser considerada de manera independiente a la tecnología o medios utilizados para su provisión a través de las redes locales, siendo su finalidad principal el establecimiento de una comunicación mediante la transmisión de voz entre partes.

ARTÍCULO 56. — *Neutralidad de red*. Se garantiza a cada usuario el derecho a acceder, utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación, servicio o protocolo a través de Internet sin ningún tipo de restricción, discriminación, distinción, bloqueo, interferencia, entorpecimiento o degradación.

ARTÍCULO 57. — *Neutralidad de red. Prohibiciones*. Los prestadores de Servicios de TIC no podrán:

a) Bloquear, interferir, discriminar, entorpecer, degradar o restringir la utilización, envío, recep- ción, ofrecimiento o acceso a cualquier contenido, aplicación, servicio o protocolo salvo orden judicial o expresa solicitud del usuario.

b) Fijar el precio de acceso a Internet en virtud de los contenidos, servicios, protocolos o aplica- ciones que vayan a ser utilizados u ofrecidos a través de los respectivos contratos.

c) Limitar arbitrariamente el derecho de un usuario a utilizar cualquier hardware o software para acceder a Internet, siempre que los mismos no dañen o perjudiquen la red.

ARTÍCULO 58. — *Velocidad Mínima de Transmisión (VMT)*. La Autoridad de Aplicación definirá, en un plazo no mayor a ciento ochenta (180) días a contar desde la entrada en vigencia de la presente ley, la Velocidad Mínima de Transmisión (VMT) que deberán posibilitar las redes de telecomunicaciones a los fines de asegurar la efectiva funcionalidad de los Servicios de TIC. Los licenciatarios de Servicios de TIC deberán proveer a sus usuarios finales, no licenciatarios de estos servicios, la velocidad fijada. La VMT deberá ser revisada con una periodicidad máxima de dos (2) años.

Título VIII

Derechos y obligaciones de los usuarios y licenciatarios de Servicios de TIC Capítulo I
Derechos y obligaciones de los usuarios de los Servicios de TIC ARTÍCULO 59. — *Derechos*. El usuario de los Servicios de TIC tiene derecho a:

a) Tener acceso al Servicio de TIC en condiciones de igualdad, continuidad, regularidad y cali- dad.

b) Ser tratado por los licenciatarios con cortesía, corrección y diligencia.

c) Tener acceso a toda la información relacionada con el ofrecimiento o prestación de los servi- cios.

d) Elegir libremente el licenciatario, los servicios y los equipos o aparatos necesarios para su prestación, siempre que estén debidamente homologados.

e) Presentar, sin requerimientos previos innecesarios, peticiones y quejas ante el licenciatario y recibir una respuesta respetuosa, oportuna, adecuada y veraz.

f) La protección de los datos personales que ha suministrado al licenciatario, los cuales no pue- den ser utilizados para fines distintos a los autorizados, de conformidad con las disposiciones vigentes.

g) Que el precio del servicio que recibe sea justo y razonable.

h) Los demás derechos que se deriven de la aplicación de las leyes, reglamentos y normas apli- cables.

ARTÍCULO 60. — *Obligaciones*. El usuario de los Servicios de TIC tiene las siguientes obliga- ciones:

a) Abonar oportunamente los cargos por los servicios recibidos, de conformidad con los precios contratados o las tarifas establecidas.

b) Mantener las instalaciones domiciliarias a su cargo de manera adecuada a las normas técni- cas vigentes.

c) No alterar los equipos terminales cuando a consecuencia de ello puedan causar daños o inter- ferencias que degraden la calidad del servicio, absteniéndose de efectuar un uso indebido del servicio.

d) Permitir el acceso del personal de los licenciatarios y de la Autoridad de Aplicación, quienes deberán estar debidamente identificados a los efectos de realizar todo tipo de trabajo o verifica- ción necesaria.

e) Respetar las disposiciones legales, reglamentarias y las condiciones generales de contrata- ción y las demás obligaciones que se deriven de la aplicación de las leyes, reglamentos y nor- mas aplicables.

Capítulo II

Derechos y obligaciones de los licenciatarios

ARTÍCULO 61. — *Derechos*. Los licenciatarios de Servicios de TIC tienen derecho a:

a) Usar y proteger sus redes e instalaciones empleadas en la prestación del Servicio de TIC.

b) Instalar sus redes y equipos en todo el territorio nacional de acuerdo a lo establecido en la presente ley y demás normativa aplicable en materia de uso del suelo, subsuelo, espacio aéreo, bienes de dominio público y privado.

c) A los demás derechos que se deriven de la presente ley y su reglamentación.

ARTÍCULO 62. — *Obligaciones*. Los licenciatarios de Servicios de TIC tienen las siguientes obli- gaciones:

a) Brindar el servicio bajo los principios de igualdad, continuidad y regularidad, cumpliendo con los niveles de calidad establecidos en la normativa vigente.

b) No incluir en los contratos cláusulas que restrinjan o condicionen en modo alguno a los usua- rios la libertad de elección de otro licenciatario o que condicionen la rescisión del mismo o la desconexión de cualquier servicio adicional contratado.

c) Garantizar que los grupos sociales específicos, las personas con discapacidad, entre ellos los usuarios con problemas graves de visión o discapacidad visual, los hipoacúsicos y los impedidos del habla, las personas mayores y los usuarios con necesidades sociales especiales tengan ac- ceso al servicio en condiciones equiparables al resto de los usuarios, de conformidad con lo es- tablecido en la normativa específica.

d) Contar con mecanismos gratuitos de atención a los usuarios de conformidad con lo dispuesto por la Autoridad de Aplicación.

e) Proporcionar al usuario información en idioma nacional y en forma clara, necesaria, veraz, oportuna, suficiente, cierta y gratuita, que no induzca a error y contenga toda la información so- bre las características esenciales del servicio que proveen al momento de la oferta, de la cele- bración del contrato, durante su ejecución y con posterioridad a su finalización.

f) Garantizar a los usuarios la confidencialidad de los mensajes transmitidos y el secreto de las comunicaciones.

g) Brindar toda la información solicitada por las autoridades competentes, especialmente la in- formación contable o económica con la periodicidad y bajo las formas que se establezcan, así como aquella que permita conocer las condiciones de prestación del servicio y toda otra informa- ción que pueda ser considerada necesaria para el cumplimiento de las funciones.

h) Disponer del equipamiento necesario para posibilitar que la Autoridad de Aplicación pueda efectuar sus funciones; encontrándose obligados a permitir el acceso de la Autoridad de Aplica- ción a sus instalaciones y brindar la información que le sea requerida por ella.

i) Atender los requerimientos en materia de defensa nacional y de seguridad pública formulados por las autoridades competentes.

j) Respetar los derechos que les corresponden a los usuarios de acuerdo con la normativa apli- cable.

k) Cumplir con las obligaciones previstas en las respectivas licencias, el marco regulatorio co- rrespondiente y las decisiones que dicte la Autoridad de Aplicación.

l) Actuar bajo esquemas de competencia leal y efectiva de conformidad con la normativa vigente.

m) Cumplir las demás obligaciones que se deriven de la presente ley y reglamentación vigente.

Título IX Régimen de sanciones

ARTÍCULO 63. — *Reglamentación*. La Autoridad de Aplicación reglamentará el régimen sancio- natorio de conformidad a los principios y disposiciones del presente Título.

ARTÍCULO 64. — *Procedimiento*. El procedimiento administrativo para la instrucción del sumario y la aplicación de sanciones será dictado por la Autoridad de Aplicación. Supletoriamente será de aplicación la Ley Nacional de Procedimientos Administrativos 19.549.

ARTÍCULO 65. — *Medidas previas al inicio del proceso sancionatorio*. Mediante el dictado del correspondiente acto administrativo, sin intervención previa y de conformidad al proceso que determine la Autoridad de Aplicación, podrá disponerse el cese de la presunta actividad infracto- ra cuando existan razones de imperiosa urgencia basadas en los siguientes supuestos:

a) Afectación del funcionamiento de los servicios de Seguridad Nacional, Defensa Civil y de Emergencias.

b) Exposición a peligro de la vida humana.

c) Interferencia a otras redes o Servicios de TIC y a las que se produzcan sobre las

frecuencias utilizadas por el Servicio de Radionavegación Aeronáutica y el Servicio Móvil Aeronáutico.

Habiendo facultades concurrentes con otra autoridad competente, se dará traslado a ésta luego de materializada la medida precautoria.

ARTÍCULO 66. — *Medidas cautelares en el proceso sancionatorio*. Mediante el dictado del co- rrespondiente acto administrativo emanado en el ámbito de la Autoridad de Aplicación, podrán adoptarse medidas cautelares consistentes en:

a) El cese inmediato de emisiones radioeléctricas no autorizadas.

b) El cese inmediato de cualquier otra actividad presuntamente infractora que pudiere ocasionar un daño irreparable a los usuarios finales del servicio.

c) El precintado de equipos o instalaciones afectados a la prestación de Servicios de TIC.

Las medidas cautelares que se hubiesen dictado cesarán en sus efectos como tales cuando se dicte la medida que ponga fin al procedimiento sancionatorio.

ARTÍCULO 67. — *Tipos de sanciones*. El incumplimiento de las obligaciones establecidas en la presente ley, sus reglamentaciones, las licencias, autorizaciones o permisos de uso dará lugar a la aplicación de las siguientes sanciones:

a) Apercibimiento.

b) Multa.

c) Suspensión de la comercialización.

d) Clausura.

e) Inhabilitación.

f) Comiso de equipos y materiales utilizados para la prestación de los servicios.

g) Decomiso.

h) Caducidad de la licencia, del registro o revocatoria de la autorización o del permiso. ARTÍCULO 68. — *Accesoria de inhabilitación*. La sanción de caducidad de la licencia inhabilitará
a la titular sancionada y a los integrantes de sus órganos directivos por el término de cinco (5)
años para ser titulares de licencias, socios o administradores de licenciatarias.

ARTÍCULO 69. — *Carácter formal*. Las infracciones tendrán carácter formal y se configurarán con independencia del dolo o culpa de los titulares de las licencias, registros o permisos y de las personas por quienes aquéllos deban responder.

ARTÍCULO 70. — *Graduación de sanciones*. La sanción que se imponga ante la

verificación de una infracción se graduará teniendo en cuenta la gravedad de la infracción, la capacidad econó- mica del infractor y el grado de afectación al interés público.

A los efectos de la determinación de sanciones, se considerarán como situaciones agravantes a tener en consideración:

a) El carácter continuado del hecho pasible de sanción.

b) La afectación del servicio.

c) La obtención de beneficios económicos por parte del infractor.

d) La clandestinidad.

e) La falta de homologación o certificación de los aparatos o equipos empleados.

ARTÍCULO 71. — *Atenuantes*. Se considerarán como situaciones atenuantes a tener en consi- deración:

a) Haber reconocido en el curso del procedimiento la existencia de la infracción.

b) Haber subsanado por iniciativa propia la situación de infracción y resarcido en forma integral los daños que pudiere haber causado.

ARTÍCULO 72. — *Decomiso*. En aquellos casos en los que se detecte la prestación de Servicios de TIC en infracción a las licencias, permisos, autorizaciones, homologaciones o habilitaciones dispuestas en la presente ley o que por cualquier medio invadan u obstruyan las vías generales de comunicación, se perderán en beneficio del Estado nacional los bienes, instalaciones y equi- pos empleados en la comisión de dichas infracciones.

ARTÍCULO 73. — *Obligación de reintegrar*. La aplicación de sanciones será independiente de la obligación de reintegrar o compensar las tarifas, precios o cargos indebidamente percibidos de los usuarios, con actualización e intereses, o de indemnizar los perjuicios ocasionados a los usuarios, al Estado, o a los terceros por la infracción.

ARTÍCULO 74. — *Reiteración*. El acto sancionatorio firme en sede administrativa constituirá an- tecedente válido a los fines de la reiteración de la infracción. Se considerará reiteración cuando se le haya aplicado sanción en relación con la misma obligación dentro de los últimos veinticua- tro (24) meses.

ARTÍCULO 75. — *Publicidad*. La Autoridad de Aplicación determinará los casos en los cuales, a cargo del infractor, procederá la publicación de las sanciones aplicadas.

ARTÍCULO 76. — *Recursos*. El acto por el cual se aplique la sanción establecida, agotará la vía administrativa a los efectos del artículo 23 de la Ley Nacional de Procedimientos Administrativos 19.549, sin perjuicio de la procedencia del recurso de alzada por el que pueda optar el recurren- te.

Agotada la vía administrativa, procederá el recurso en sede judicial conforme al artículo 4° de la presente. Su interposición no tendrá efecto suspensivo, salvo en el caso de la sanción

de cadu- cidad de la licencia.

Título X Autoridades Capítulo I

Autoridad Federal de Tecnologías de la Información y las Comunicaciones

ARTÍCULO 77 **[derogado por Dec.267/2015]**.

ARTÍCULO 78 **[derogado por Dec.267/2015]**.

ARTÍCULO 79. — *Continuación*. La Autoridad Federal de Tecnologías de la Información y las Comunicaciones creada por la presente ley será continuadora, a todos los fines y de conformi- dad con lo fijado en la presente ley, de la Secretaría de Comunicaciones y de la Comisión Na- cional de Comunicaciones creada por los decretos 1142/2003 y 1185/90 y sus posteriores modi- ficaciones.

ARTÍCULO 80. — *Funciones*. La Autoridad Federal de Tecnologías de la Información y las Co- municaciones tendrá como funciones la regulación, el control, la fiscalización y verificación en materia de las TIC en general, de las telecomunicaciones en particular, del servicio postal y to- das aquellas materias que se integren a su órbita conforme el texto de la presente ley, la norma- tiva aplicable y las políticas fijadas por el Gobierno nacional.

ARTÍCULO 81. — *Competencias*. La Autoridad Federal de Tecnologías de la Información y las Comunicaciones ejercerá las siguientes competencias:

a) Regular y promover la competencia y el desarrollo eficiente de las telecomunicaciones y los servicios digitales en el ámbito de las atribuciones que le confiere esta ley y demás disposiciones legales aplicables.

b) La regulación, promoción y supervisión del uso, aprovechamiento y explotación del espectro radioeléctrico, los recursos orbitales, los servicios satelitales, las redes de telecomunicaciones y la prestación de los servicios de telecomunicaciones y tecnologías digitales, así como del acceso a la infraestructura activa y pasiva y otros insumos o facilidades esenciales, sin perjuicio de las atribuciones que corresponden a otras autoridades en los términos de la legislación correspon- diente.

c) Regular en materia de lineamientos técnicos relativos a la infraestructura y los equipos que se conecten a las redes de telecomunicaciones, así como en materia de homologación y evaluación de la conformidad de dicha infraestructura y equipos.

d) Resolver sobre el otorgamiento, la prórroga, la revocación de licencias, registros permisos y autorizaciones, así como la autorización de cesiones o cambios de control accionario, titularidad u operación de sociedades relacionadas con concesiones en materia de telecomunicaciones y servicios previstos en esta ley.

e) Adoptar, en su caso, las acciones y medidas necesarias que garanticen la continuidad en la prestación de los servicios de telecomunicaciones y servicios de comunicación audiovisual cuando la autoridad le dé aviso de la existencia de causas de terminación por revocación o res- cate de concesiones, disolución o quiebra de las sociedades

concesionarias.

f) Planear, fijar, instrumentar y conducir las políticas y programas de cobertura universal y cober- tura social de conformidad con lo establecido en esta ley.

g) Promover y regular el acceso a las tecnologías de la información y comunicación y a los servi- cios de telecomunicaciones, incluido el de banda ancha e Internet, en condiciones de competen- cia efectiva.

h) Expedir disposiciones administrativas de carácter general, planes técnicos fundamentales, lineamientos, modelos de costos, procedimientos de evaluación de la conformidad, procedimien- tos de homologación y certificación y ordenamientos técnicos en materia de telecomunicaciones y servicios de comunicación audiovisual; así como demás disposiciones para el cumplimiento de lo dispuesto en esta ley.

i) Formular y publicar sus programas de trabajo.

j) Elaborar, publicar y mantener actualizado el Cuadro Nacional de Atribución de Frecuencias.

k) Emitir disposiciones, lineamientos o resoluciones en materia de interoperabilidad e interco- nexión de las redes públicas de telecomunicaciones, a efecto de asegurar la libre competencia y concurrencia en el mercado.

l) Resolver y establecer los términos y condiciones de interconexión que no hayan podido con- venir los concesionarios respecto de sus redes públicas de telecomunicaciones conforme a lo previsto en la presente ley.

ll) Emitir lineamientos de carácter general para el acceso y, en su caso, uso compartido de la infraestructura activa y pasiva, en los casos que establece esta ley.

m) Resolver los desacuerdos de compartición de infraestructura entre licenciatarios conforme a lo dispuesto en esta ley.

n) Resolver los desacuerdos que se susciten entre licenciatarios de redes de telecomunicacio- nes.

ñ) Resolver las solicitudes de interrupción parcial o total, por hechos fortuitos o causas de fuerza mayor de las vías generales de comunicación en materia de telecomunicaciones.

o) Resolver sobre el cambio o rescate de bandas de frecuencia.

p) Determinar la existencia de actores con poder significativo de mercado e imponer las medidas necesarias para evitar que se afecte la competencia y la libre concurrencia en cada uno de los mercados de esta ley.

q) Declarar la existencia o inexistencia de condiciones de competencia efectiva en el sector de que se trate y, en su caso, la extinción de las obligaciones impuestas a los actores con poder significativo de mercado.

r) Determinar, autorizar, registrar y publicar las tarifas de los servicios en las condiciones previs- tas en esta ley.

s) Requerir a los sujetos regulados por esta ley la información y documentación, incluso aquella generada por medios electrónicos, ópticos o de cualquier otra tecnología, necesarios para el ejercicio de sus atribuciones.

t) Coordinar acciones con las autoridades del Poder Ejecutivo, provinciales y municipales.

u) Imponer las sanciones por infracciones a las disposiciones legales, reglamentarias o adminis- trativas.

v) Las demás que le confiera esta ley y otras disposiciones legales o administrativas.
ARTÍCULO 82 **[derogado por Dec.267/2015]**.
ARTÍCULO 83 **[derogado por Dec.267/2015]**.

ARTÍCULO 84 **[derogado por Dec.267/2015]**.

Capítulo II

Consejo Federal de Tecnologías de las Telecomunicaciones y la Digitalización ARTÍCULO 85 **[derogado por Dec.267/2015]**.
ARTÍCULO 86 **[derogado por Dec.267/2015]**.

ARTÍCULO 87. — *Transferencias*. Transfiérense bajo la órbita de competencias de la Autoridad de Aplicación de la presente ley los siguientes organismos, empresas, programas y proyectos:

- Secretaría de Comunicaciones (SECOM).
- Comisión Nacional de Comunicaciones (CNC).
- Argentina Soluciones Satelitales S.A. (ARSAT).
- Correo Oficial de la República Argentina S.A. (CORASA).
- Argentina Conectada.

Capítulo III

Comisión Bicameral de Promoción y Seguimiento de la Comunicación Audiovisual, las Tecnolog- ías de las Telecomunicaciones y la Digitalización

ARTÍCULO 88. — Sustitúyese el Capítulo III del Título II de la ley 26.522, el que quedará redac- tado de la siguiente forma:

Capítulo III

Comisión Bicameral de Promoción y Seguimiento de la Comunicación Audiovisual, las Tecnolog- ías de las Telecomunicaciones y la Digitalización

Artículo 18.- *Comisión Bicameral*. Créase en el ámbito del Congreso de la Nación, la Comisión Bicameral de Promoción y Seguimiento de la Comunicación Audiovisual, las Tecnologías de las Telecomunicaciones y la Digitalización, que tendrá el carácter de Comisión Permanente.

La Comisión Bicameral se integrará por ocho (8) senadores y ocho (8) diputados nacionales, según resolución de cada Cámara. Dictará su propio reglamento.

De entre sus miembros elegirán un (1) presidente, un (1) vicepresidente y un (1) secretario; car- gos que serán ejercidos anualmente en forma alternada por un representante de cada Cámara.

La comisión tendrá las siguientes competencias:

a) Proponer al Poder Ejecutivo nacional, los candidatos para la designación de tres (3) miembros del directorio de la Autoridad Federal de Servicios de Comunicación Audiovisual, y de tres (3) miembros del directorio de Radio y Televisión Argentina Sociedad del Estado y del titular de la Defensoría del Público de Servicios de Comunicación Audiovisual por resolución conjunta de ambas Cámaras.

b) Proponer al Poder Ejecutivo nacional, los candidatos para la designación de tres (3) miembros del directorio de la Autoridad Federal de Tecnologías de la Información y las Comunicaciones por resolución conjunta de ambas Cámaras.

c) Recibir y evaluar el informe presentado por el Consejo Consultivo Honorario de los Medios Públicos e informar a sus respectivos cuerpos orgánicos, dando a publicidad sus conclusiones.

d) Velar por el cumplimiento de las disposiciones referidas a Radio y Televisión Argentina Socie- dad del Estado.

e) Evaluar el desempeño de los miembros del directorio de la Autoridad Federal de Servicios de Comunicación Audiovisual y del Defensor del Público.

f) Evaluar el desempeño de los miembros del directorio de la Autoridad Federal de Tecnologías de la Información y las Comunicaciones.

g) Dictaminar sobre la remoción por incumplimiento o mal desempeño de su cargo al Defensor del Público; en un procedimiento en el que se haya garantizado en forma amplia el derecho de defensa, debiendo la resolución que se adopta al respecto estar debidamente fundada.

Título XI

Cláusulas transitorias y disposiciones finales

ARTÍCULO 89. — La ley 19.798 y sus modificatorias sólo subsistirá respecto de aquellas

dispo- siciones que no se opongan a las previsiones de la presente ley.

ARTÍCULO 90. — *Alcance. Decreto 62/90*. La definición del artículo 6° inciso c) de la presente comprende los aspectos de la definición establecida en el Pliego de Bases y Condiciones para el Concurso Público Internacional para la Privatización de la Prestación del Servicio de Telecomu- nicaciones aprobado mediante el decreto 62/90.

ARTÍCULO 91. — *Integración del FFSU*. Establécese que en virtud de lo dispuesto por las Cláu- sulas 11.1 y 11.2 del Contrato de Fideicomiso de Administración del Fondo Fiduciario del Servi- cio Universal decreto 558/08, los recursos del mismo previstos en el artículo 8° del Anexo III del decreto 764/00 y sus modificatorios quedarán integrados al Fondo del Servicio Universal creado por artículo 21 de la presente ley, en las condiciones que determine la Autoridad de Aplicación.

ARTÍCULO 92. — *Derogación*. Derógase el decreto 764/00 y sus modificatorios, sin perjuicio de lo cual mantendrá su vigencia en todo lo que no se oponga a la presente ley durante el tiempo que demande a la Autoridad de Aplicación dictar los reglamentos concernientes al Régimen de Licencias para Servicios de TIC, al Régimen Nacional de Interconexión, al Régimen General del Servicio Universal y al Régimen sobre la Administración, Gestión y Control del Espectro Radio- eléctrico.

ARTÍCULO 93. — *Régimen de transición*. *Licencias*. A los actuales licenciatarios, operadores, prestadores y autorizados bajo el régimen instituido en el decreto 764/00 y sus modificatorios se les aplicará el régimen previsto en la presente.

Al momento de la sanción de la presente, y sin más trámite, los títulos habilitantes actualmente denominados ‘Licencia Única de Servicios de Telecomunicaciones’ serán considerados a todos los efectos ‘Licencia Única Argentina Digital’, sin mutar en su contenido, alcance y efectos.

La Autoridad de Aplicación podrá establecer regímenes y programas especiales tendientes a la regularización de situaciones de prestación cuyos responsables no cuenten con la licencia co- rrespondiente, contemplando a tal efecto la situación particular de cada actor involucrado garan- tizando la continuidad de la prestación de los Servicios de TIC, sin que ello implique saneamien- to de situación irregular alguna.

ARTÍCULO 94 **[texto vigente a partir del Dec. 267/2015]**.- Los prestadores del Servicio Básico Te- lefónico, cuya licencia ha sido concedida en los términos del Decreto N° 62/90 y de los puntos 1 y 2 del artículo 5º del Decreto N° 264/98, así como los del Servicio de Telefonía Móvil con licen- cia otorgada conforme el pliego de bases y condiciones aprobado por Resolución del entonces MINISTERIO DE ECONOMÍA Y OBRAS Y SERVICIOS PÚBLICOS Nº 575/93 y ratificado por Decreto N° 1461/93, sólo podrán prestar el servicio de Radiodifusión por suscripción, mediante vínculo físico y/o mediante vínculo radioeléctrico, transcurridos DOS (2) años contados a partir del 1° de enero de 2016. El ENACOM podrá extender dicho plazo por UN (1) año más.

ARTÍCULO 95 **[texto vigente a partir del Dec. 267/2015]**.- No podrán ser titulares de un registro de Radiodifusión por suscripción mediante vínculo físico o mediante vínculo radioeléctrico los titulares o accionistas que posean el DIEZ POR CIENTO (10%) o más de las acciones o cuotas partes que conforman la voluntad social de una persona de existencia

ideal titular o accionista de una persona de existencia ideal a quien el estado nacional, provincial o municipal le haya otorgado la licencia, concesión o permiso para la prestación de un servicio público.

No será aplicable lo dispuesto en el párrafo anterior a:

(i) Las personas de existencia ideal sin fines de lucro a quien el estado nacional, provincial o municipal le haya otorgado la licencia, concesión o permiso para la prestación de un servicio público;

(ii) Los sujetos mencionados en el artículo 94, que sólo podrán prestar el servicio transcurrido el plazo allí previsto.

En el caso de los incisos (i) y (ii) referidos y a los efectos de la obtención de un registro de Ra- diodifusión por Suscripción, la explotación del registro quedará sujeta a las condiciones que se indican a continuación y las demás que establezca la reglamentación.

Si al momento de solicitar el registro existe otro prestador en la misma área de servicio, el ENACOM deberá, en cada caso concreto, realizar una evaluación integral de la solicitud que contemple el interés de la población y dar publicidad de la solicitud en el BOLETÍN OFICIAL y en la página web del ENACOM. En caso de presentarse oposición por parte de otro titular de un registro de Radiodifusión por Suscripción en la misma área de prestación, el ENACOM de- berá solicitar un dictamen a la autoridad de aplicación de la Ley N° 25.156 que establezca las condiciones de prestación del solicitante. El plazo para presentar oposiciones es de TREINTA
(30) días hábiles desde la fecha de publicación de la solicitud en el Boletín Oficial. Este párrafo se aplicará sólo para el caso del inciso (i) anterior.

No será aplicable lo dispuesto en el párrafo anterior a las personas de existencia ideal sin fines de lucro que exclusivamente presten servicio público de TIC.

En todos los casos, las personas previstas en los apartados (i) y (ii) anteriores que obtengan el registro de servicios de Radiodifusión por suscripción en los términos y condiciones fijadas en este artículo deberán cumplir con las siguientes obligaciones:

a) Conformar una unidad de negocio a los efectos de la prestación del servicio de comunica- ción audiovisual y llevarla en forma separada de la unidad de negocio del servicio público del que se trate;

b) Llevar una contabilidad separada y facturar por separado las prestaciones correspondientes al servicio licenciado;

c) No incurrir en prácticas anticompetitivas tales como las prácticas atadas y los subsidios cru- zados con fondos provenientes del servicio público hacia el servicio licenciado;

d) Facilitar -cuando sea solicitado- a los competidores en los servicios licenciados el acceso a su propia infraestructura de soporte, en especial postes, mástiles y ductos, en condiciones de mercado. En los casos en que no existiera acuerdo entre las partes, se deberá pedir interven- ción al ENACOM;

e) No incurrir en prácticas anticompetitivas en materia de derechos de exhibición de los conteni- dos a difundir por sus redes y facilitar un porcentaje creciente a determinar por el ENACOM a la distribución de contenidos de terceros independientes.

f) Respetar las incumbencias y encuadramientos profesionales de los trabajadores en las distin- tas actividades que se presten.

ARTÍCULO 96 **[texto vigente a partir del Dec. 267/2015]**. — Las restricciones y obligaciones es- tablecidas en los artículos 9°, 94 y 95 de la presente ley, serán también de aplicación a:

(i) Los titulares de cualquier participación social directa o indirecta en los sujetos mencionados en el artículo 94;

(ii) Cualquier persona en la que los sujetos mencionados en el artículo 94 tengan participación social directa o indirecta; y

(iii) Los contratos de colaboración, de organización o participativo, con comunidad de fin, que no sean sociedad, constituidos por o en los que participen los sujetos mencionados en el artículo 94 y en los incisos (i) y (ii) precedentes, incluidos los negocios en participación, agrupaciones de colaboración, uniones transitorias y consorcios de cooperación.

ARTÍCULO 97. — *Vigencia*. La presente ley entrará en vigencia a partir del día de su publicación en el Boletín Oficial de la República Argentina.

ARTÍCULO 98. — Comuníquese al Poder Ejecutivo nacional.

DADA EN LA SALA DE SESIONES DEL CONGRESO ARGENTINO, EN BUENOS AIRES, A LOS DIECISEIS DIAS DEL MES DE DICIEMBRE DEL AÑO DOS MIL CATORCE.

— REGISTRADA BAJO EL Nº 27.078 —

AMADO BOUDOU. — JULIAN A. DOMINGUEZ. — Lucas Chedrese. — Juan H. Estrada.

Texto digitalizado y revisado de acuerdo a los originales del Boletín Oficial, por el personal del Centro de Información Técnica del Ente Nacional de Comunicaciones.

3. Германия

3.1. Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz - ITSiG)

(http://www.buzer.de/gesetz/11682/a193756.htm)

G. v. 17.07.2015 BGBl. I S. 1324 (Nr. 31); zuletzt geändert durch Artikel 5 Abs. 8 G. v. 18.07.2016 BGBl. I S. 1666
Geltung ab 25.07.2015, abweichend siehe Artikel 11
9 Änderungen | Drucksachen / Entwurf / Begründung | wird in 12 Vorschriften zitiert

Artikel 1 Änderung des BSI-Gesetzes

Artikel 1 wird in 2 Vorschriften zitiert und ändert mWv. 25. Juli 2015 BSIG § 1, § 2, § 3, § 4, § 5, § 7, § 7a (neu), § 8, § 8a (neu), § 8b (neu), § 8c (neu), § 8d (neu), § 10, § 13 (neu), § 14 (neu)

Das BSI-Gesetz vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 3 Absatz 7 des Gesetzes vom7. August 2013 (BGBl. I S. 3154) geändert worden ist, wird wie folgt geändert:

1. § 1 wird wie folgt gefasst:

„§ 1 Bundesamt für Sicherheit in der Informationstechnik

Der Bund unterhält ein Bundesamt für Sicherheit in der Informationstechnik (Bundesamt) als Bundesoberbehörde. Das Bundesamt ist zuständig für die Informationssicherheit auf nationaler Ebene. Es untersteht dem Bundesministerium des Innern."

2. Dem § 2 wird folgender Absatz 10 angefügt:
„(10) Kritische Infrastrukturen im Sinne dieses Gesetzes sind Einrichtungen, Anlagen oder Teile davon, die

1. den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und
2. von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.
Die Kritischen Infrastrukturen im Sinne dieses Gesetzes werden durch die Rechtsverordnung nach § 10Absatz 1 näher bestimmt."

3. § 3 wird wie folgt geändert:

a) Absatz 1 Satz 2 wird wie folgt geändert:

aa) In Nummer 2 werden die Wörter „zur Wahrung ihrer Sicherheitsinteressen erforderlich ist" durch die Wörter „erforderlich ist, sowie für Dritte, soweit dies zur Wahrung ihrer Sicherheitsinteressen erforderlich ist" ersetzt.
bb) In Nummer 15 werden die Wörter „kritischen Informationsinfrastrukturen" durch die Wörter „Sicherheit in der Informationstechnik Kritischer Infrastrukturen" und der Punkt am Ende durch ein Semikolon ersetzt.
cc) Die folgenden Nummern 16 und 17 werden angefügt:

„16. Aufgaben als zentrale Stelle im Bereich der Sicherheit in der Informationstechnik im Hinblick auf die Zusammenarbeit mit den zuständigen Stellen im Ausland, unbeschadet besonderer Zuständigkeiten anderer Stellen;

17. Aufgaben nach den §§ 8a und 8b als zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen."

b) Folgender Absatz 3 wird angefügt:
„(3) Das Bundesamt kann Betreiber Kritischer Infrastrukturen auf deren Ersuchen bei der Sicherung ihrer Informationstechnik beraten und unterstützen oder auf qualifizierte Sicherheitsdienstleister verweisen."

4. Die Überschrift von § 4 wird wie folgt gefasst:

„§ 4 Zentrale Meldestelle für die Sicherheit in der Informationstechnik des Bundes".
4a.
§ 5 Absatz 1 wird wie folgt geändert:

a) Satz 4 wird wie folgt gefasst:

„Die Bundesbehörden sind verpflichtet, das Bundesamt bei Maßnahmen nach Satz 1 zu unterstützen und hierbei den Zugang des Bundesamtes zu behördeninternen Protokolldaten nach Satz 1 Nummer 1 sowie Schnittstellendaten nach Satz 1 Nummer 2 sicherzustellen."

b) Folgender Satz wird angefügt:

„Protokolldaten der Bundesgerichte dürfen nur in deren Einvernehmen erhoben werden."

5. § 7 Absatz 1 Satz 1 wird durch die folgenden Sätze ersetzt:
“Zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 14 kann das Bundesamt

1. die folgenden Warnungen an die Öffentlichkeit oder an die betroffenen Kreise richten:

a) Warnungen vor Sicherheitslücken in informationstechnischen Produkten und Diensten,
b) Warnungen vor Schadprogrammen und
c) Warnungen im Falle eines Verlustes von oder eines unerlaubten Zugriffs auf Daten;

2.Sicherheitsmaßnahmen sowie den Einsatz bestimmter Sicherheitsprodukte empfehlen.
Das Bundesamt kann zur Wahrnehmung der Aufgaben nach Satz 1 Dritte einbeziehen, wenn dies für eine wirksame und rechtzeitige Warnung erforderlich ist."
6.

Nach § 7 wird folgender § 7a eingefügt:

„§ 7a Untersuchung der Sicherheit in der Informationstechnik
(1) Das Bundesamt kann zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 14 und 17 auf dem Markt bereitgestellte oder zur Bereitstellung auf dem Markt vorgesehene informationstechnische Produkte und Systeme untersuchen. Es kann sich hierbei der Unterstützung Dritter bedienen, soweit berechtigte Interessen des Herstellers der betroffenen Produkte und Systeme dem nicht entgegenstehen.

(2) Die aus den Untersuchungen gewonnenen Erkenntnisse dürfen nur zur Erfüllung der Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 14 und 17 genutzt werden. Das Bundesamt darf seine Erkenntnisse weitergeben und veröffentlichen, soweit dies zur Erfüllung dieser Aufgaben erforderlich ist. Zuvor ist dem Hersteller der betroffenen Produkte und Systeme mit angemessener Frist Gelegenheit zur Stellungnahme zu geben."

6a.
§ 8 Absatz 1 wird wie folgt gefasst:
„(1) Das Bundesamt erarbeitet Mindeststandards für die Sicherheit der Informationstechnik des Bundes. Das Bundesministerium des Innern kann im Benehmen mit dem IT-Rat diese Mindeststandards ganz oder teilweise als allgemeine Verwaltungsvorschriften für alle Stellen des Bundes erlassen. Das Bundesamt berät die Stellen des Bundes auf Ersuchen bei der Umsetzung und Einhaltung der Mindeststandards. Für die in § 2 Absatz 3 Satz 2 genannten Gerichte und Verfassungsorgane haben die Vorschriften nach diesem Absatz empfehlenden Charakter."

7. Nach § 8 werden die folgenden §§ 8a bis 8d eingefügt:

„§ 8a Sicherheit in der Informationstechnik Kritischer Infrastrukturen
(1) Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei soll der Stand der Technik eingehalten werden. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.

(2) Betreiber Kritischer Infrastrukturen und ihre Branchenverbände können branchenspezifische Sicherheitsstandards zur Gewährleistung der Anforderungen nach Absatz 1 vorschlagen. Das Bundesamt stellt auf Antrag fest, ob diese geeignet sind, die Anforderungen nach Absatz 1 zu gewährleisten. Die Feststellung erfolgt

1. im Benehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe,
2. im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde.

(3) Die Betreiber Kritischer Infrastrukturen haben mindestens alle zwei Jahre die Erfüllung der Anforderungen nach Absatz 1 auf geeignete Weise nachzuweisen. Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen. Die Betreiber übermitteln dem Bundesamt eine Aufstellung der durchgeführten Audits, Prüfungen oder Zertifizierungen

einschließlich der dabei aufgedeckten Sicherheitsmängel. Das Bundesamt kann bei Sicherheitsmängeln verlangen:

1. die Übermittlung der gesamten Audit-, Prüfungs- oder Zertifizierungsergebnisse und
2. im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der Sicherheitsmängel.

(4) Das Bundesamt kann zur Ausgestaltung des Verfahrens der Sicherheitsaudits, Prüfungen und Zertifizierungen nach Absatz 3 Anforderungen an die Art und Weise der Durchführung, an die hierüber auszustellenden Nachweise sowie fachliche und organisatorische Anforderungen an die prüfende Stelle nach Anhörung von Vertretern der betroffenen Betreiber und der betroffenen Wirtschaftsverbände festlegen.

§ 8b Zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen

(1) Das Bundesamt ist die zentrale Meldestelle für Betreiber Kritischer Infrastrukturen in Angelegenheiten der Sicherheit in der Informationstechnik.

(2) Das Bundesamt hat zur Wahrnehmung dieser Aufgabe

1. die für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik wesentlichen Informationen zu sammeln und auszuwerten, insbesondere Informationen zu Sicherheitslücken, zu Schadprogrammen, zu erfolgten oder versuchten Angriffen auf die Sicherheit in der Informationstechnik und zu der dabei beobachteten Vorgehensweise,
2. deren potentielle Auswirkungen auf die Verfügbarkeit der Kritischen Infrastrukturen in Zusammenarbeit mit den zuständigen Aufsichtsbehörden und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe zu analysieren,
3. das Lagebild bezüglich der Sicherheit in der Informationstechnik der Kritischen Infrastrukturen kontinuierlich zu aktualisieren und
4. unverzüglich

a) die Betreiber Kritischer Infrastrukturen über sie betreffende Informationen nach den Nummern 1 bis 3,
b) die zuständigen Aufsichtsbehörden und die sonst zuständigen Behörden des Bundes über die zur Erfüllung ihrer Aufgaben erforderlichen Informationen nach den Nummern 1 bis 3 sowie
c) die zuständigen Aufsichtsbehörden der Länder oder die zu diesem Zweck dem Bundesamt von den Ländern als zentrale Kontaktstellen benannten Behörden über die zur Erfüllung ihrer Aufgaben erforderlichen Informationen nach den Nummern 1 bis 3
zu unterrichten.

(3) Die Betreiber Kritischer Infrastrukturen haben dem Bundesamt binnen sechs Monaten nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 eine Kontaktstelle für die Kommunikationsstrukturen nach § 3 Absatz 1 Satz 2 Nummer 15 zu benennen. Die Betreiber haben sicherzustellen, dass sie hierüber jederzeit erreichbar sind. Die Übermittlung von Informationen durch das Bundesamt nach Absatz 2 Nummer 4 erfolgt an diese Kontaktstelle.

(4) Betreiber Kritischer Infrastrukturen haben erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen

1. führen können oder
2. geführt haben,
über die Kontaktstelle unverzüglich an das Bundesamt zu melden. Die Meldung muss Angaben zu der Störung sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik, der Art der betroffenen Einrichtung oder Anlage sowie zur Branche des Betreibers enthalten. Die Nennung des Betreibers ist nur dann erforderlich, wenn die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt hat.

(5) Zusätzlich zu ihrer Kontaktstelle nach Absatz 3 können Betreiber Kritischer Infrastrukturen, die dem gleichen Sektor angehören, eine gemeinsame übergeordnete Ansprechstelle benennen. Wurde eine solche benannt, erfolgt der Informationsaustausch zwischen den Kontaktstellen und dem Bundesamt in der Regel über die gemeinsame Ansprechstelle.

(6) Soweit erforderlich kann das Bundesamt vom Hersteller der betroffenen informationstechnischen Produkte und Systeme die Mitwirkung an der Beseitigung oder Vermeidung einer Störung nach Absatz 4 verlangen. Satz 1 gilt für Störungen bei Betreibern und Genehmigungsinhabern im Sinne von § 8c Absatz 3 entsprechend.

(7) Soweit im Rahmen dieser Vorschrift personenbezogene Daten erhoben, verarbeitet oder genutzt werden, ist eine über die vorstehenden Absätze hinausgehende Verarbeitung und Nutzung zu anderen Zwecken unzulässig. § 5 Absatz 7 Satz 3 bis 8 ist entsprechend anzuwenden. Im Übrigen sind die Regelungen des Bundesdatenschutzgesetzes anzuwenden.

§ 8c Anwendungsbereich
(1) Die §§ 8a und 8b sind nicht anzuwenden auf Kleinstunternehmen im Sinne der Empfehlung 2003/361/EC der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (ABl. L 124 vom 20.5.2003, S. 36). Artikel 3 Absatz 4 der Empfehlung ist nicht anzuwenden.

(2) § 8a ist nicht anzuwenden auf

1. Betreiber Kritischer Infrastrukturen, soweit sie ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen,
2. Betreiber von Energieversorgungsnetzen oder Energieanlagen im Sinne desEnergiewirtschaftsgesetzes vom 7. Juli 2005 (BGBl. I S. 1970, 3621), das zuletzt durch Artikel 3 des Gesetzes vom 17. Juli 2015 (BGBl. I S. 1324) geändert worden ist, in der jeweils geltenden Fassung,
3. Genehmigungsinhaber nach § 7 Absatz 1 des Atomgesetzes in der Fassung der Bekanntmachung vom15. Juli 1985 (BGBl. I S. 1565), das zuletzt durch Artikel 2 des Gesetzes vom 17. Juli 2015 (BGBl. I S. 1324) geändert worden ist, in der jeweils geltenden Fassung für den Geltungsbereich der Genehmigung sowie
4. sonstige Betreiber Kritischer Infrastrukturen, soweit sie auf Grund von Rechtsvorschriften Anforderungen erfüllen müssen, die mit den Anforderungen nach § 8a vergleichbar oder weitergehend sind.

(3) § 8b Absatz 3 bis 5 ist nicht anzuwenden auf

1. Betreiber Kritischer Infrastrukturen, soweit sie ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen,
2. Betreiber von Energieversorgungsnetzen oder Energieanlagen im Sinne des Energiewirtschaftsgesetzes,
3. Genehmigungsinhaber nach § 7 Absatz 1 des Atomgesetzes für den Geltungsbereich der Genehmigung sowie
4. sonstige Betreiber Kritischer Infrastrukturen, die auf Grund von Rechtsvorschriften Anforderungen erfüllen müssen, die mit den Anforderungen nach § 8b Absatz 3 bis 5 vergleichbar oder weitergehend sind.

§ 8d Auskunftsverlangen
(1) Das Bundesamt kann Dritten auf Antrag Auskunft zu den im Rahmen von § 8a Absatz 2 und 3 erhaltenen Informationen sowie zu den Meldungen nach § 8b Absatz 4 nur erteilen, wenn schutzwürdige Interessen des betroffenen Betreibers Kritischer Infrastrukturen dem nicht entgegenstehen und durch die Auskunft keine Beeinträchtigung wesentlicher Sicherheitsinteressen zu erwarten ist. Zugang zu personenbezogenen Daten wird nicht gewährt.

(2) Zugang zu den Akten des Bundesamtes in Angelegenheiten nach den §§ 8a und 8b wird nur Verfahrensbeteiligten gewährt und dies nach Maßgabe von § 29 des Verwaltungsverfahrensgesetzes."

8. § 10 wird wie folgt geändert:

a) Dem Absatz 1 wird folgender Absatz 1 vorangestellt:
„(1) Das Bundesministerium des Innern bestimmt durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, nach Anhörung von Vertretern der Wissenschaft, der betroffenen Betreiber und der betroffenen Wirtschaftsverbände im Einvernehmen mit dem Bundesministerium für Wirtschaft und Energie, dem Bundesministerium der Justiz und für Verbraucherschutz, dem Bundesministerium der Finanzen, dem Bundesministerium für Arbeit und Soziales, dem Bundesministerium für Ernährung und Landwirtschaft, dem Bundesministerium für Gesundheit, dem Bundesministerium für Verkehr und digitale Infrastruktur, dem Bundesministerium der Verteidigung und dem Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit unter Festlegung der in den jeweiligen Sektoren im Hinblick auf § 2 Absatz 10 Satz 1 Nummer 2 wegen ihrer Bedeutung als kritisch anzusehenden Dienstleistungen und deren als bedeutend anzusehenden Versorgungsgrads, welche Einrichtungen, Anlagen oder Teile davon als Kritische Infrastrukturen im Sinne dieses Gesetzes gelten. Der nach Satz 1 als bedeutend anzusehende Versorgungsgrad ist anhand von branchenspezifischen Schwellenwerten für jede wegen ihrer Bedeutung als kritisch anzusehende Dienstleistung im jeweiligen Sektor zu bestimmen. Zugang zu Akten, die die Erstellung oder Änderung dieser Verordnung betreffen, wird nicht gewährt."

b) Der bisherige Absatz 1 wird Absatz 2 und die Wörter „Wirtschaft und Technologie durch Rechtsverordnung" werden durch die Wörter „Wirtschaft und Energie durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf," ersetzt.
c) Der bisherige Absatz 2 wird Absatz 3 und in Satz 3 werden nach dem Wort „Rechtsverordnung" ein Komma und die Wörter „die nicht der Zustimmung des Bundesrates bedarf," eingefügt.

9. Die folgenden §§ 13 und 14 werden angefügt:

„§ 13 Berichtspflichten
(1) Das Bundesamt unterrichtet das Bundesministerium des Innern über seine Tätigkeit.

(2) Die Unterrichtung nach Absatz 1 dient auch der Aufklärung der Öffentlichkeit durch das Bundesministerium des Innern über Gefahren für die Sicherheit in der Informationstechnik, die mindestens einmal jährlich in einem zusammenfassenden Bericht erfolgt. § 7 Absatz 1 Satz 3 und 4 ist entsprechend anzuwenden.

§ 14 Bußgeldvorschriften
(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 8a Absatz 1 Satz 1 in Verbindung mit einer Rechtsverordnung nach § 10 Absatz 1 Satz 1 eine dort genannte Vorkehrung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig trifft,
2. einer vollziehbaren Anordnung nach § 8a Absatz 3 Satz 4

a) Nummer 1 oder
b) Nummer 2
zuwiderhandelt,
3. entgegen § 8b Absatz 3 Satz 1 in Verbindung mit einer Rechtsverordnung nach § 10 Absatz 1 Satz 1 eine Kontaktstelle nicht oder nicht rechtzeitig benennt oder
4. entgegen § 8b Absatz 4 Satz 1 Nummer 2 eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht.
(2) Die Ordnungswidrigkeit kann in den Fällen des Absatzes 1 Nummer 2 Buchstabe b mit einer Geldbuße bis zu hunderttausend Euro, in den übrigen Fällen des Absatzes 1 mit einer Geldbuße bis zu fünfzigtausend Euro geahndet werden.

(3) Verwaltungsbehörde im Sinne des § 36 Absatz 1 Nummer 1 des Gesetzes über Ordnungswidrigkeitenist das Bundesamt."

Artikel 2 Änderung des Atomgesetzes

Artikel 2 wird in 2 Vorschriften zitiert und ändert mWv. 25. Juli 2015 AtG § 44b (neu)

Nach § 40 des Atomgesetzes in der Fassung der Bekanntmachung vom 15. Juli 1985 (BGBl. I S. 1565), das zuletzt durch Artikel 2 Absatz 14 des Gesetzes vom 1. April 2015 (BGBl. I S. 434) geändert worden ist, wird folgender § 44b eingefügt:

„§ 44b Meldewesen für die Sicherheit in der Informationstechnik

Genehmigungsinhaber nach den §§ 6, 7 und 9 haben Beeinträchtigungen ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einer Gefährdung oder Störung der nuklearen Sicherheit der betroffenen kerntechnischen Anlage oder Tätigkeit führen können oder bereits geführt haben, unverzüglich an das Bundesamt für Sicherheit in der Informationstechnik als zentrale Meldestelle zu melden. § 8b Absatz 1, 2 und 7 des BSI-Gesetzes sind entsprechend anzuwenden. Die Meldung muss Angaben zu der Störung sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, und der betroffenen Informationstechnik enthalten. Das Bundesamt für Sicherheit in

der Informationstechnik leitet diese Meldungen unverzüglich an die für die nukleare Sicherheit und Sicherung zuständigen Genehmigungs- und Aufsichtsbehörden des Bundes und der Länder weiter."

Artikel 3 Änderung des Energiewirtschaftsgesetzes

Artikel 3 wird in 2 Vorschriften zitiert und ändert mWv. 25. Juli 2015 EnWG § 11, § 21e, § 21f, § 21i, § 59

Das Energiewirtschaftsgesetz vom 7. Juli 2005 (BGBl. I S. 1970, 3621), das zuletzt durch Artikel 6 des Gesetzes vom 21. Juli 2014 (BGBl. I S. 1066) geändert worden ist, wird wie folgt geändert:

1. § 11 wird wie folgt geändert:

a) Absatz 1a wird wie folgt geändert:

aa) In Satz 1 werden nach dem Wort „Datenverarbeitungssysteme," die Wörter „die der Netzsteuerung dienen" durch die Wörter „die für einen sicheren Netzbetrieb notwendig sind" ersetzt.

bb) Nach Satz 2 wird folgender Satz eingefügt:

„Der Katalog der Sicherheitsanforderungen enthält auch Regelungen zur regelmäßigen Überprüfung der Erfüllung der Sicherheitsanforderungen."
cc) In dem neuen Satz 4 werden die Wörter „wird vermutet" durch die Wörter „liegt vor" ersetzt.
dd) Der neue Satz 6 wird wie folgt gefasst:

„Zu diesem Zwecke kann die Regulierungsbehörde nähere Bestimmungen zu Format, Inhalt und Gestaltung der Dokumentation nach Satz 4 treffen."
b) Nach Absatz 1a werden die folgenden Absätze 1b und 1c eingefügt:
„(1b) Betreiber von Energieanlagen, die durch Inkrafttreten der Rechtsverordnung gemäß § 10Absatz 1 des BSI-Gesetzes vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 8 des Gesetzes vom 17. Juli 2015 (BGBl. I S. 1324) geändert worden ist, in der jeweils geltenden Fassung als Kritische Infrastruktur bestimmt wurden und an ein Energieversorgungsnetz angeschlossen sind, haben binnen zwei Jahren nach Inkrafttreten der Rechtsverordnung gemäß § 10 Absatz 1 des BSI-Gesetzes einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme zu gewährleisten, die für einen sicheren Anlagenbetrieb notwendig sind. Die Regulierungsbehörde erstellt hierzu im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik einen Katalog von Sicherheitsanforderungen und veröffentlicht diesen. Für Telekommunikations- und elektronische Datenverarbeitungssysteme von Anlagen nach § 7Absatz 1 des Atomgesetzes haben Vorgaben auf Grund des Atomgesetzes Vorrang. Die für die nukleare Sicherheit zuständigen Genehmigungs- und Aufsichtsbehörden des Bundes und der Länder sind bei der Erarbeitung des Katalogs von Sicherheitsanforderungen zu beteiligen. Der Katalog von Sicherheitsanforderungen enthält auch Regelungen zur regelmäßigen Überprüfung der Erfüllung der Sicherheitsanforderungen. Ein angemessener

Schutz des Betriebs von Energieanlagen im Sinne von Satz 1 liegt vor, wenn dieser Katalog eingehalten und dies vom Betreiber dokumentiert worden ist. Die Einhaltung kann von der Bundesnetzagentur überprüft werden. Zu diesem Zwecke kann die Regulierungsbehörde nähere Bestimmungen zu Format, Inhalt und Gestaltung der Dokumentation nach Satz 6 treffen.

(1c) Betreiber von Energieversorgungsnetzen und Energieanlagen, die durch Inkrafttreten der Rechtsverordnung gemäß § 10 Absatz 1 des BSI-Gesetzes als Kritische Infrastruktur bestimmt wurden, haben dem Bundesamt für Sicherheit in der Informationstechnik unverzüglich erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu melden, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit des Energieversorgungsnetzes oder der betreffenden Energieanlage führen können oder bereits geführt haben. Die Meldung muss Angaben zu der Störung sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache und der betroffenen Informationstechnik, enthalten. Die Nennung des Betreibers ist nur dann erforderlich, wenn die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt hat. Das Bundesamt für Sicherheit in der Informationstechnik hat die Meldungen unverzüglich an die Bundesnetzagentur weiterzuleiten. Das Bundesamt für Sicherheit in der Informationstechnik und die Bundesnetzagentur haben sicherzustellen, dass die unbefugte Offenbarung der ihnen nach Satz 1 zur Kenntnis gelangten Angaben ausgeschlossen wird. Zugang zu den Akten des Bundesamtes für Sicherheit in der Informationstechnik sowie zu den Akten der Bundesnetzagentur in Angelegenheiten nach den §§ 11a bis 11c wird nicht gewährt. § 29 desVerwaltungsverfahrensgesetzes bleibt unberührt. § 8d Absatz 1 des BSI-Gesetzes ist entsprechend anzuwenden."

2. § 21e Absatz 5 wird wie folgt geändert:

a) In Satz 1 in dem Satzteil vor Nummer 1 werden nach den Wörtern „dürfen noch" die Wörter „bis zum Zeitpunkt, den eine Rechtsverordnung nach § 21i Absatz 1 Nummer 11 bestimmt, mindestens jedoch" eingefügt und wird die Angabe „2014" durch die Angabe „2015" ersetzt.
b) Satz 3 wird aufgehoben.
3. § 21f Absatz 2 wird wie folgt geändert:

a) In Satz 1 werden nach den Wörtern „können noch" die Wörter „bis zum Zeitpunkt, den eine Rechtsverordnung nach § 21i Absatz 1 Nummer 11 bestimmt, mindestens jedoch" eingefügt und wird die Angabe „2014" durch die Angabe „2015" ersetzt.
b) Satz 2 wird aufgehoben.

4. In § 21i Absatz 1 Nummer 11 werden die Wörter „und eine Verlängerung der genannten Frist" gestrichen.

5. In § 59 Absatz 1 Satz 2 werden nach dem Wort „Erstellung" die Wörter „und Überprüfung" eingefügt und wird nach der Angabe „§ 11 Absatz 1a" die Angabe „Satz 2" durch die Angabe „und 1b" ersetzt.

Artikel 4 Änderung des Telemediengesetzes

Artikel 4 wird in 1 Vorschrift zitiert und ändert mWv. 25. Juli 2015 TMG § 13, § 16

Das Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179, 251), das zuletzt durch Artikel 2 Absatz 16 des Gesetzes vom 1. April 2015 (BGBl. I S. 434) geändert worden ist, wird wie folgt geändert:

1.
§ 13 wird wie folgt geändert:
a)
Nach Absatz 6 wird folgender Absatz 7 eingefügt:
„(7) Diensteanbieter haben, soweit dies technisch möglich und wirtschaftlich zumutbar ist, im Rahmen ihrer jeweiligen Verantwortlichkeit für geschäftsmäßig angebotene Telemedien durch technische und organisatorische Vorkehrungen sicherzustellen, dass

1.
kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist und
2.
diese

a)
gegen Verletzungen des Schutzes personenbezogener Daten und
b)
gegen Störungen, auch soweit sie durch äußere Angriffe bedingt sind,
gesichert sind. Vorkehrungen nach Satz 1 müssen den Stand der Technik berücksichtigen. Eine Maßnahme nach Satz 1 ist insbesondere die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens."
b)
Der bisherige Absatz 7 wird Absatz 8.
2.
In § 16 Absatz 2 Nummer 3 werden nach den Wörtern „§ 13 Abs. 4 Satz 1 Nr. 1 bis 4 oder 5" die Wörter „oder Absatz 7 Satz 1 Nummer 1 oder Nummer 2 Buchstabe a" eingefügt.

→ Artikel 6

Artikel 5 Änderung des Telekommunikationsgesetzes

Artikel 5 wird in 1 Vorschrift zitiert und ändert mWv. 25. Juli 2015 TKG § 100, § 109, § 109a, § 149

Das Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), das zuletzt durch Artikel 22 des Gesetzes vom 25. Juli 2014 (BGBl. I S. 1266) geändert worden ist, wird wie folgt geändert:

1.
In der Inhaltsübersicht wird die Angabe zu § 109a wie folgt gefasst:

„§ 109a Daten- und Informationssicherheit".
2.
§ 100 Absatz 1 wird wie folgt gefasst:

„(1) Soweit erforderlich, darf der Diensteanbieter die Bestandsdaten und Verkehrsdaten der Teilnehmer und Nutzer erheben und verwenden, um Störungen oder Fehler an Telekommunikationsanlagen zu erkennen, einzugrenzen oder zu beseitigen. Dies gilt auch für Störungen, die zu einer Einschränkung der Verfügbarkeit von Informations- und Kommunikationsdiensten oder zu einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer führen können."

3.
§ 109 wird wie folgt geändert:

a)
Nach Absatz 2 Satz 2 wird folgender Satz eingefügt:

„Bei Maßnahmen nach Satz 2 ist der Stand der Technik zu berücksichtigen."
b)
Absatz 4 Satz 7 wird durch die folgenden Sätze ersetzt:

„Die Bundesnetzagentur überprüft regelmäßig die Umsetzung des Sicherheitskonzepts. Die Überprüfung soll mindestens alle zwei Jahre erfolgen."
c)
Absatz 5 wird wie folgt gefasst:
„(5) Wer ein öffentliches Telekommunikationsnetz betreibt oder öffentlich zugängliche Telekommunikationsdienste erbringt, hat der Bundesnetzagentur unverzüglich Beeinträchtigungen von Telekommunikationsnetzen und -diensten mitzuteilen, die

1.
zu beträchtlichen Sicherheitsverletzungen führen oder
2.
zu beträchtlichen Sicherheitsverletzungen führen können.
Dies schließt Störungen ein, die zu einer Einschränkung der Verfügbarkeit der über diese Netze erbrachten Dienste oder einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer führen können. Die Meldung muss Angaben zu der Störung sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache und zu der betroffenen Informationstechnik enthalten. Kommt es zu einer beträchtlichen Sicherheitsverletzung, kann die Bundesnetzagentur einen detaillierten Bericht über die Sicherheitsverletzung und die ergriffenen Abhilfemaßnahmen verlangen. Soweit es sich um Sicherheitsverletzungen handelt, die die Informationstechnik betreffen, leitet die Bundesnetzagentur die eingegangenen Meldungen sowie die Informationen zu den ergriffenen Abhilfemaßnahmen unverzüglich an das Bundesamt für Sicherheit in der Informationstechnik weiter. Erforderlichenfalls unterrichtet die Bundesnetzagentur die nationalen Regulierungsbehörden der anderen Mitgliedstaaten der Europäischen Union und die Europäische Agentur für Netz- und Informationssicherheit über die Sicherheitsverletzungen. Die Bundesnetzagentur kann die Öffentlichkeit unterrichten oder die nach Satz 1 Verpflichteten zu dieser Unterrichtung auffordern, wenn sie zu dem Schluss gelangt, dass die Bekanntgabe der Sicherheitsverletzung im öffentlichen Interesse liegt. § 8d des BSI-Gesetzes gilt entsprechend. Die Bundesnetzagentur legt der Europäischen Kommission, der Europäischen Agentur für Netz- und Informationssicherheit und dem Bundesamt für Sicherheit in der Informationstechnik einmal pro Jahr einen zusammenfassenden Bericht über die eingegangenen Meldungen und die ergriffenen Abhilfemaßnahmen vor."

d)
In Absatz 6 Satz 1 wird das Wort „Benehmen" durch das Wort „Einvernehmen" ersetzt.
e)
Folgender Absatz 8 wird angefügt:
„(8) Über aufgedeckte Mängel bei der Erfüllung der Sicherheitsanforderungen in der Informationstechnik sowie die in diesem Zusammenhang von der Bundesnetzagentur geforderten Abhilfemaßnahmen unterrichtet die Bundesnetzagentur unverzüglich das Bundesamt für Sicherheit in der Informationstechnik."

4.
§ 109a wird wie folgt geändert:

a)
Die Überschrift wird wie folgt gefasst:

„§ 109a Daten- und Informationssicherheit".
b)
Nach Absatz 3 wird folgender Absatz 4 eingefügt:
„(4) Werden dem Diensteanbieter nach Absatz 1 Störungen bekannt, die von Datenverarbeitungssystemen der Nutzer ausgehen, so hat er die Nutzer, soweit ihm diese bereits bekannt sind, unverzüglich darüber zu benachrichtigen. Soweit technisch möglich und zumutbar, hat er die Nutzer auf angemessene, wirksame und zugängliche technische Mittel hinzuweisen, mit denen sie diese Störungen erkennen und beseitigen können."

c) Der bisherige Absatz 4 wird Absatz 5.
5. § 149 Nummer 21a wird wie folgt gefasst:

„21a. entgegen § 109 Absatz 5 Satz 1 Nummer 1 eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,".

Artikel 6 Änderung des Bundesbesoldungsgesetzes

Artikel 6 wird in 1 Vorschrift zitiert und ändert mWv. 25. Juli 2015 BBesG Anlage I, BBesO A/B Besoldungsgruppe B 6, Besoldungsgruppe B 7

Die Anlage I des Bundesbesoldungsgesetzes in der Fassung der Bekanntmachung vom 19. Juni 2009 (BGBl. I S. 1434), das zuletzt durch Artikel 2 des Gesetzes vom 13. Mai 2015 (BGBl. I S. 706) geändert worden ist, wird wie folgt geändert:

1.
In der Gliederungseinheit „Besoldungsgruppe B 6" wird die Angabe „Präsident des Bundesamtes für Sicherheit in der Informationstechnik" gestrichen.
2.
In der Gliederungseinheit „Besoldungsgruppe B 7" wird nach der Angabe „Präsident des Bildungszentrums der Bundeswehr" folgende Angabe eingefügt:

„Präsident des Bundesamtes für Sicherheit in der Informationstechnik".

Artikel 7 Änderung des Bundeskriminalamtgesetzes

Artikel 7 wird in 1 Vorschrift zitiert und ändert mWv. 25. Juli 2015 BKAG § 4

§ 4 Absatz 1 Satz 1 Nummer 5 des Bundeskriminalamtgesetzes vom 7. Juli 1997 (BGBl. I S. 1650), das zuletzt durch Artikel 3 des Gesetzes vom 20. Juni 2013 (BGBl. I S. 1602) geändert worden ist, wird wie folgt geändert:

1.
In dem Satzteil vor Buchstabe a wird die Angabe „§ 303b" durch die Wörter „den §§ 202a, 202b, 202c, 263a, 303a und 303b" ersetzt.
2.
In Buchstabe b werden vor dem Wort „sicherheitsempfindliche" die Wörter „Behörden oder Einrichtungen des Bundes oder" eingefügt.

Artikel 8 (aufgehoben)
Artikel 8 hat 1 frühere Fassung und wird in 3 Vorschriften zitiert

Text in der Fassung des Artikels 5 Gesetz zur Aktualisierung der Strukturreform des Gebührenrechts des Bundes G. v. 18. Juli 2016 BGBl. I S. 1666 m.W.v. 23. Juli 2016

Artikel 9 Änderung des Gesetzes zur Strukturreform des Gebührenrechts des Bundes
Artikel 9 wird in 1 Vorschrift zitiert und ändert mWv. 25. Juli 2015 BGebGEG Artikel 3

Artikel 3 Absatz 7 des Gesetzes zur Strukturreform des Gebührenrechts des Bundes vom 7. August 2013 (BGBl. I S. 3154) wird aufgehoben.

Artikel 10 Evaluierung

Artikel 1 Nummer 2, 7 und 8 sind vier Jahre nach Inkrafttreten der Rechtsverordnung nach Artikel 1 Nummer 8 unter Einbeziehung eines wissenschaftlichen Sachverständigen, der im Einvernehmen mit dem Deutschen Bundestag bestellt wird, zu evaluieren.

Artikel 11 Inkrafttreten

Artikel 11 hat 1 frühere Fassung und wird in 1 Vorschrift zitiert
Dieses Gesetz tritt vorbehaltlich des Satzes 2 am Tag nach der Verkündung in Kraft.

Schlussformel

Die verfassungsmäßigen Rechte des Bundesrates sind gewahrt.

Das vorstehende Gesetz wird hiermit ausgefertigt. Es ist im Bundesgesetzblatt zu verkünden.

Der Bundespräsident

Joachim Gauck

Die Bundeskanzlerin

Dr. Angela Merkel

Der Bundesminister des Innern

Thomas de Maizière

3.2. Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung - BSI-KritisV) vom 22. April 2016 (BGBl. I S. 958)

(https://www.gesetze-im-internet.de/bundesrecht/bsi-kritisv/gesamt.pdf)

Eingangsformel

Auf Grund des § 10 Absatz 1 des BSI-Gesetzes vom 14. August 2009 (BGBl. I S. 2821), der zuletzt durch die Artikel 1 Nummer 8 des Gesetzes vom 17. Juli 2015 (BGBl. I S. 1324) geändert worden ist, verordnet das Bundesministerium des Innern im Einvernehmen mit dem Bundesministerium für Wirtschaft und Energie, dem Bundesministerium der Justiz und für Verbraucherschutz, dem Bundesministerium der Finanzen, dem Bundesministerium für Arbeit und Soziales, dem Bundesministerium für Ernährung und Landwirtschaft, dem Bundesministerium für Gesundheit, dem Bundesministerium für Verkehr und digitale Infrastruktur, dem Bundesministerium der Verteidigung und dem Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit nach Anhörung der beteiligten Kreise:

§ 1 Begriffsbestimmungen

Im Sinne dieser Verordnung ist oder sind
1.
Anlagen
a)
Betriebsstätten und sonstige ortsfeste Einrichtungen, die für die Erbringung einer kritischen Dienstleistung notwendig sind.
b)
Maschinen, Geräte und sonstige ortsveränderliche Einrichtungen, die für die Erbringung einer kritischen Dienstleistung notwendig sind.
Einer Anlage sind alle vorgesehenen Anlagenteile und Verfahrensschritte zuzurechnen, die zum Betrieb notwendig sind, sowie Nebeneinrichtungen, die mit den Anlagenteilen und Verfahrensschritten in einem betriebstechnischen Zusammenhang stehen und die für die Erbringung einer kritischen Dienstleistung notwendig sind.
2.
Betreiber
eine natürliche oder juristische Person, die unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände bestimmenden Einfluss auf die Beschaffenheit und den Betrieb einer Anlage oder Teilen davon ausübt.
3.
Kritische Dienstleistung
eine Dienstleistung zur Versorgung der Allgemeinheit in den Sektoren nach den §§ 2 bis 5, deren Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen oder zu Gefährdungen der öffentlichen Sicherheit führen würde.
4.
Versorgungsgrad
ein Wert, mittels dessen der Beitrag einer Anlage oder Teilen davon im jeweiligen Sektor zur Versorgung der Allgemeinheit mit einer kritischen Dienstleistung bestimmt wird.
5.

Schwellenwert
ein Wert, bei dessen Erreichen oder dessen Überschreitung der Versorgungsgrad einer Anlage oder Teilen davon als bedeutend im Sinne von § 10 Absatz 1 Satz 1 des BSI-Gesetzes anzusehen ist.

§ 2 Sektor Energie

(1) Wegen ihrer besonderen Bedeutung für das Funktionieren des Gemeinwesens sind im Sektor Energie kritische Dienstleistungen im Sinne des § 10 Absatz 1 Satz 1 des BSI-Gesetzes:

1.
die Versorgung der Allgemeinheit mit Elektrizität (Stromversorgung);

2.
die Versorgung der Allgemeinheit mit Gas (Gasversorgung);

3.
die Versorgung der Allgemeinheit mit Kraftstoff und Heizöl (Kraftstoff- und Heizölversorgung);

4.
die Versorgung der Allgemeinheit mit Fernwärme (Fernwärmeversorgung).

(2) Die Stromversorgung und Gasversorgung werden in den Bereichen Erzeugung, Übertragung und Verteilung von Strom sowie Förderung, Transport und Verteilung von Gas erbracht.

(3) Die Kraftstoff- und Heizölversorgung wird in den Bereichen Rohölförderung und Produktherstellung, Öltransport sowie Kraftstoff- und Heizölverteilung erbracht.

(4) Die Fernwärmeversorgung wird in den Bereichen Erzeugung von Fernwärme und Verteilung von Fernwärme erbracht.

(5) Im Sektor Energie sind Kritische Infrastrukturen solche Anlagen oder Teile davon, die

1.
den in Anhang 1 Teil 3 Spalte B genannten Kategorien zuzuordnen sind und die für die Stromversorgung, Gasversorgung, Kraftstoff- und Heizölversorgung und Fernwärmeversorgung in den Bereichen erforderlich sind, die in den Absätzen 2 bis 4 genannt werden, und

2.
den Schwellenwert nach Anhang 1 Teil 3 Spalte D erreichen oder überschreiten.

§ 3 Sektor Wasser

(1) Wegen ihrer besonderen Bedeutung für das Funktionieren des Gemeinwesens sind im Sektor Wasser kritische Dienstleistungen im Sinne des § 10 Absatz 1 Satz 1 des BSI-Gesetzes:

1.
die Versorgung der Allgemeinheit mit Trinkwasser (Trinkwasserversorgung);

2.
die Beseitigung von Abwasser der Allgemeinheit (Abwasserbeseitigung).

(2) Die Trinkwasserversorgung wird in den Bereichen Gewinnung, Aufbereitung und Verteilung von Trinkwasser erbracht.

(3) Die Abwasserbeseitigung wird in den Bereichen Siedlungsentwässerung sowie Abwasserbehandlung und Gewässereinleitung erbracht.

(4) Im Sektor Wasser sind Kritische Infrastrukturen solche Anlagen oder Teile davon, die

1.

den in Anhang 2 Teil 3 Spalte B genannten Kategorien zuzuordnen sind und die für die Trinkwasserversorgung und Abwasserbeseitigung in den Bereichen erforderlich sind, die in den Absätzen 2 und 3 genannt werden, und
2.
den Schwellenwert nach Anhang 2 Teil 3 Spalte D erreichen oder überschreiten.

§ 4 Sektor Ernährung
(1) Wegen ihrer besonderen Bedeutung für das Funktionieren des Gemeinwesens ist im Sektor Ernährung die Versorgung der Allgemeinheit mit Lebensmitteln (Lebensmittelversorgung) kritische Dienstleistung im Sinne des § 10 Absatz 1 Satz 1 des BSI-Gesetzes.
(2) Die Lebensmittelversorgung wird in den Bereichen Lebensmittelproduktion und -verarbeitung sowie Lebensmittelhandel erbracht.
(3) Im Sektor Ernährung sind Kritische Infrastrukturen solche Anlagen oder Teile davon, die
1.
den in Anhang 3 Teil 3 Spalte B genannten Kategorien zuzuordnen sind und die für die Lebensmittelversorgung in den Bereichen erforderlich sind, die in Absatz 2 genannt werden, und
2.
den Schwellenwert nach Anhang 3 Teil 3 Spalte D erreichen oder überschreiten.

§ 5 Sektor Informationstechnik und Telekommunikation
(1) Wegen ihrer besonderen Bedeutung für das Funktionieren des Gemeinwesens sind im Sektor Informationstechnik und Telekommunikation kritische Dienstleistungen im Sinne des § 10 Absatz 1 Satz 1 des BSI-Gesetzes:
1.
Sprach- und Datenübertragung;
2.
Datenspeicherung und -verarbeitung.
(2) Die Sprach- und Datenübertragung wird in den Bereichen Zugang, Übertragung, Vermittlung und Steuerung erbracht.
(3) Die Datenspeicherung und -verarbeitung wird in den Bereichen Housing, IT-Hosting und Vertrauensdienste erbracht.
(4) Im Sektor Informationstechnik und Telekommunikation sind Kritische Infrastrukturen solche Anlagen oder Teile davon, die
1.
den in Anhang 4 Teil 3 Spalte B genannten Kategorien zuzuordnen sind und die für die Sprach- und Datenübertragung sowie Datenspeicherung und -verarbeitung in den Bereichen erforderlich sind, die in den Absätzen 2 und 3 genannt werden, und
2.
den Schwellenwert nach Anhang 4 Teil 3 Spalte D erreichen oder überschreiten.

§ 6 Evaluierung
Vier Jahre nach Inkrafttreten dieser Rechtsverordnung sind unter Beteiligung der in § 10 Absatz 1 Satz 1 des BSI-Gesetzes genannten Ressorts zu evaluieren
1.
die Festlegung der kritischen Dienstleistungen und Bereiche,
2.
die Festlegung der Anlagenkategorien, die für die Erbringung der kritischen Dienstleistungen erforderlich sind, und

3.
die Bestimmung der Schwellenwerte.

§ 7 Inkrafttreten
Diese Verordnung tritt am Tag nach der Verkündung in Kraft.

Anhang 1 (zu § 1 Nummer 4 und 5, § 2 Absatz 5 Nummer 1 und 2) Anlagenkategorien und Schwellenwerte im Sektor Energie
(Fundstelle: BGBl. I 2016,960 - 962)

Teil 1
Grundsätze und Fristen
1.
Für die in Teil 3 Spalte B genannten Anlagenkategorien gelten vorrangig die Begriffsbestimmungen nach § 3 des Energiewirtschaftsgesetzes und nach § 2 des Kraft-Wärme-Kopplungsgesetzes in der jeweils geltenden Fassung.
2.
Eine Anlage, die einer in Teil 3 Spalte B genannten Anlagenkategorie zuzuordnen ist, gilt zum 1. April des Kalenderjahres, das auf das Kalenderjahr folgt, in dem ihr Versorgungsgrad den in Teil 3 Spalte D genannten Schwellenwert erstmals erreicht oder überschreitet, als Kritische Infrastruktur. Hat der Versorgungsgrad einer Anlage den in Teil 3 Spalte D genannten Schwellenwert im Kalenderjahr 2015 erstmals erreicht oder überschritten, gilt die Anlage mit Inkrafttreten dieser Verordnung als Kritische Infrastruktur.
3.
Der Betreiber hat den Versorgungsgrad seiner Anlage für das zurückliegende Kalenderjahr bis zum 31. März des Folgejahres zu ermitteln.
4.
Ist der Versorgungsgrad für die Anlagenkategorie des Teils 3 Nummer 4.2.1 unmittelbar anhand der Anzahl angeschlossener Haushalte zu ermitteln, ist der Versorgungsgrad zum 30. Juni des zurückliegenden Kalenderjahres maßgeblich.
5.
Ist der Versorgungsgrad für die Anlagenkategorien des Teils 3 Nummer 1.1 anhand der Kapazität (installierte Netto-Nennleistung) einer Anlage zu ermitteln, ist auf den rechtlich und tatsächlich möglichen Betriebsumfang der durch denselben Betreiber betriebenen Anlage abzustellen.
6.
Stehen mehrere Anlagen derselben Art in einem engen räumlichen und betrieblichen Zusammenhang (gemeinsame Anlage) und erreichen oder überschreiten die in Teil 3 Spalte D genannten Schwellenwerte zusammen, gilt die gemeinsame Anlage als Kritische Infrastruktur. Ein enger räumlicher und betrieblicher Zusammenhang ist gegeben, wenn die Anlagen
a)
auf demselben Betriebsgelände liegen,
b)
mit gemeinsamen Betriebseinrichtungen verbunden sind,
c)
einem vergleichbaren technischen Zweck dienen und
d)
unter gemeinsamer Leitung stehen.
Teil 2

Berechnungsformeln zur Ermittlung der Schwellenwerte

7.

Der für die Anlagenkategorien des Teils 3 Nummer 1.1.1 bis 1.1.5, 1.2.1 sowie 1.3.1 genannte Schwellenwert ist unter Annahme eines Durchschnittsverbrauchs von 7 375 kWh pro versorgter Person pro Jahr und eines Regelschwellenwertes von 500 000 versorgten Personen wie folgt berechnet:

3 700 GWh/Jahr ≈ 7 375 kWh/Jahr x 500 000

Die durchschnittliche elektrische Arbeit zur Versorgung von 500 000 Personen im Jahr entspricht im Falle der Nummern 1.1.1 bis 1.1.5 sowie 1.3.2 einer installierten Netto-Nennleistung von:

$$420\ \text{MW} \approx \frac{3\,700\ \text{GWh/Jahr}}{8\,760\ \text{h/Jahr}}$$

8.

Der für die Anlagenkategorien des Teils 3 Nummer 2 genannte Schwellenwert ist unter Annahme eines Durchschnittsverbrauchs von 10 380 kWh pro versorgter Person pro Jahr und eines Regelschwellenwertes von 500 000 versorgten Personen wie folgt berechnet:

5 190 GWh/Jahr = 10 380 kWh/Jahr x 500 000

9.

Der für die Anlagenkategorien des Teils 3 Nummer 3.1.2, 3.2.2 und 3.3 genannte Schwellenwert ist unter Annahme einer durchschnittlichen Produktionsmenge von 0,84 Tonnen Kraftstoff zur Versorgung einer Person pro Jahr und eines Regelschwellenwertes von 500 000 versorgten Personen wie folgt berechnet:

420 000 t/Jahr = 0,84 t/Jahr x 500 000

10.

Der für die Anlagenkategorien des Teils 3 Nummer 3.1.2 und 3.2.2 genannte Schwellenwert ist unter Annahme einer durchschnittlichen Produktionsmenge von 1,24 Tonnen leichtem Heizöl zur Versorgung einer Person pro Jahr und eines Regelschwellenwertes von 500 000 versorgten Personen wie folgt berechnet:

620 000 t/Jahr = 1,24 t/Jahr x 500 000

11.

Der für die Anlagenkategorien des Teils 3 Nummer 3.1.1, 3.2.1 und 3.2.2 benannte Schwellenwert ist unter Annahme einer durchschnittlichen Produktionsmenge von 1,24 Tonnen leichtem Heizöl zur Versorgung einer Person pro Jahr und damit einer durchschnittlichen Gesamtproduktionsmenge von 620 000 Tonnen leichtem Heizöl für 500 000 versorgte Personen sowie unter der Annahme, dass aus einer Tonne Rohöl etwa 0,14 Tonnen leichtes Heizöl hergestellt werden, wie folgt berechnet:

$$4\,400\,000\ \text{t/Jahr} \approx \frac{620\,000\ \text{t/Jahr}}{0{,}14}$$

12.

Der für die Anlagenkategorien des Teils 3 Nummer 4.1.1 und 4.1.2 genannte Schwellenwert ist unter Annahme eines Durchschnittsverbrauchs einer Person pro Jahr von 4,528 MWh und eines Regelschwellenwertes von 500 000 versorgten Personen wie folgt berechnet:

2 300 GWh/Jahr ≈ 4,528 MWh/Jahr x 500 000

Teil 3
Anlagenkategorien und Schwellenwerte

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Anlagenkategorie	Bemessungskriterium	Schwellenwert
1.	**Stromversorgung**		
1.1	Stromerzeugung		
1.1.1	Erzeugungsanlage	installierte Netto-Nennleistung (elektrisch) in MW	420
1.1.2.	Erzeugungsanlage mit Wärmeauskopplung (KWK-Anlage)	installierte Netto-Nennleistung (direkt mit Wärmeauskopplung verbundene elektrische Wirkleistung bei Wärmenennleistung ohne Kondensationsanteil) in MW	420
1.1.3	Dezentrale Energieerzeugungsanlage	installierte Netto-Nennleistung (elektrisch) in MW	420
1.1.4	Speicheranlage	installierte Netto-Nennleistung (elektrisch) in MW	420
1.1.5	Anlage oder System zur Steuerung/Bündelung elektrischer Leistung	installierte Netto-Nennleistung (elektrisch) in MW	420
1.2	Stromübertragung		
1.2.1	Übertragungsnetz	Durch Letztverbraucher und Weiterverteiler entnommene Jahresarbeit in GWh/Jahr	3 700
1.2.2	Zentrale Anlage und System für den Stromhandel, soweit diese den physischen kurzfristigen Spothandel und das deutsche Marktgebiet betreffen	Handelsvolumen an der Börse in TWh/Jahr	200
1.3	Stromverteilung		
1.3.1	Verteilernetz	Durch Letztverbraucher und Weiterverteiler entnommene Jahresarbeit in GWh/Jahr	3 700
1.3.2	Messstelle	Leistung der angeschlossenen Verbrauchsstelle beziehungsweise Einspeisung in MW	420

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Anlagenkategorie	Bemessungskriterium	Schwellenwert
2.	**Gasversorgung**		
2.1	Gasförderung		
2.1.1	Gasförderanlage	Energie des geförderten Gases in GWh/Jahr	5 190
2.1.2	Gasspeicher	Entnommene Arbeit in GWh/Jahr	5 190
2.2	Gastransport		
2.2.1	Fernleitungsnetz	Durch Letztverbraucher und Weiterverteiler entnommene Jahresarbeit in GWh/Jahr	5 190
2.3	Gasverteilung		
2.3.1	Gasverteilernetz	Entnommene Arbeit in GWh/Jahr	5 190
3.	**Kraftstoff- und Heizölversorgung**		
3.1	Rohölförderung und Rohölproduktenherstellung		
3.1.1	Ölförderanlage	Gefördertes Rohöl in Tonnen/Jahr	4,4 Millionen
3.1.2	Raffinerie	Erzeugter Kraftstoff in Tonnen/Jahr oder	420 000[1]
		Erzeugtes Heizöl in Tonnen/Jahr	620 000
3.2	Öltransport		
3.2.1	Mineralölfernleitung	Transportierte Rohölmenge oder Produktenmenge in Tonnen/Jahr	4,4 Millionen
3.2.2	Öl- und Produktenlager	Umgeschlagene Rohölmenge in Tonnen/Jahr oder	4,4 Millionen
		Umgeschlagene Menge Kraftstoff in Tonnen/Jahr oder	420 000[1]
		Umgeschlagene Menge Heizöl in Tonnen/Jahr	620 000

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Anlagenkategorie	Bemessungskriterium	Schwellenwert
3.3	Kraftstoff- und Heizölverteilung		
3.3.1	Anlage und System von Aggregatoren zum Vertrieb von Kraftstoff	Verteilte Menge Kraftstoff in Tonnen/Jahr	420 000[1]
3.3.2	Tankstellennetz	Verteilte Menge Kraftstoff in Tonnen/Jahr	420 000[1]
4.	**Fernwärmeversorgung**		
4.1	Erzeugung von Fernwärme		
4.1.1	Heizwerk	Ausgeleitete Wärmeenergie in GWh/Jahr	2 300
4.1.2	Heizkraftwerk	Ausgeleitete Wärmeenergie in GWh/Jahr	2 300
4.2	Verteilung von Fernwärme		
4.2.1	Fernwärmenetz	Angeschlossene Haushalte	250 000

[1]

≈ 420 Millionen Liter

Anhang 2 (zu § 1 Nummer 4 und 5, § 3 Absatz 4 Nummer 1 und 2) Anlagenkategorien und Schwellenwerte im Sektor Wasser
(Fundstelle: BGBl. I 2016,963 - 964)

Teil 1
Grundsätze und Fristen
1.
Für die in Teil 3 Spalte B Nummer 1 genannten Anlagenkategorien gelten vorrangig die Begriffsbestimmungen nach den technischen Regeln der Deutschen Vereinigung für Wasserwirtschaft, Abwasser und Abfall e. V. (DIN EN 16323) in der jeweils geltenden Fassung. Für die in Teil 3 Spalte B Nummer 2 genannten Anlagenkategorien gelten vorrangig die Begriffsbestimmungen nach den technischen Regeln der Deutschen Vereinigung des Gas- und Wasserfachs e. V. (DIN 4046) in der jeweils geltenden Fassung.
2.
Eine Anlage, die einer in Teil 3 Spalte B genannten Anlagenkategorie zuzuordnen ist, gilt zum 1. April des Kalenderjahres, das auf das Kalenderjahr folgt, in dem ihr Versorgungsgrad den in Teil 3 Spalte D genannten Schwellenwert erstmals erreicht oder überschreitet, als Kritische Infrastruktur. Hat der Versorgungsgrad einer Anlage den in Teil 3 Spalte D genannten Schwellenwert im Kalenderjahr 2015 erstmals erreicht oder überschritten, gilt die Anlage mit Inkrafttreten dieser Verordnung als Kritische Infrastruktur.
3.
Der Betreiber hat den Versorgungsgrad seiner Anlage für das zurückliegende Kalenderjahr bis zum 31. März des Folgejahres zu ermitteln.
4.
Ist der Versorgungsgrad für die Anlagenkategorien des Teils 3 Nummer 1.1.1 bis 1.2.2 unmittelbar anhand der Anzahl versorgter Personen zu ermitteln, ist der Versorgungsgrad zum 30. Juni des zurückliegenden Kalenderjahres maßgeblich.
5.
Stehen mehrere Anlagen derselben Art in einem engen räumlichen und betrieblichen Zusammenhang (gemeinsame Anlage) und erreichen oder überschreiten die in Teil 3 Spalte D genannten Schwellenwerte zusammen, gilt die gemeinsame Anlage als Kritische Infrastruktur. Ein enger räumlicher und betrieblicher Zusammenhang ist gegeben, wenn die Anlagen
a)
auf demselben Betriebsgelände liegen,
b)
mit gemeinsamen Betriebseinrichtungen verbunden sind,
c)
einem vergleichbaren technischen Zweck dienen und
d)
unter gemeinsamer Leitung stehen.

Teil 2
Berechnungsformeln zur Ermittlung der Schwellenwerte
6.
Der für die Anlagenkategorien des Teils 3 Nummer 2.1.1 bis 2.3.2 genannte Schwellenwert ist unter Annahme eines Durchschnittsverbrauchs von 44 m^3 pro versorgter Person pro Jahr und eines Regelschwellenwertes von 500 000 versorgten Personen wie folgt berechnet:

22 Millionen m^3/Jahr = 44 m^3/Jahr x 500 000

Teil 3
Anlagenkategorien und Schwellenwerte

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Anlagenkategorie	Bemessungskriterium	Schwellenwert
1.	**Abwasserbeseitigung**		
1.1	Siedlungsentwässerung		
1.1.1	Kanalisation	Angeschlossene Einwohner	500 000
1.2	Abwasserbehandlung und Gewässereinleitung		
1.2.1	Kläranlage	Ausbaugröße in Einwohnerwerten	500 000
1.2.2	Leitzentrale	Ausbaugrößen der gesteuerten/überwachten Anlagen in Einwohnerwerten	500 000
2.	**Trinkwasserversorgung**		
2.1	Gewinnung		
2.1.1	Gewinnungsanlage	Gewonnene Wassermenge in Millionen m^3/Jahr	22
2.1.2	Wasserwerk	Wasseraufkommen in Millionen m^3/Jahr	22
2.2	Aufbereitung		
2.2.1	Aufbereitungsanlage	Aufbereitete Trinkwassermenge in Millionen m^3/Jahr	22
2.2.2	Wasserwerk	Wasseraufkommen in Millionen m^3/Jahr	22
2.3	Verteilung		
2.3.1	Wasserverteilungssystem	Verteilte Wassermenge in Millionen m^3/Jahr	22
2.3.2	Leitzentrale	Von den gesteuerten/überwachten Anlagen gewonnene, transportierte oder aufbereitete	22

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Anlagenkategorie	Bemessungskriterium	Schwellenwert
		Menge Wasser in Millionen m^3/Jahr	

Anhang 3 (zu § 1 Nummer 4 und 5, § 4 Absatz 3 Nummer 1 und 2) Anlagenkategorien und Schwellenwerte im Sektor Ernährung
(Fundstelle: BGBl. I 2016,965 - 966)

Teil 1
Grundsätze und Fristen

1.
Eine Anlage, die einer in Teil 3 Spalte B genannten Anlagenkategorie zuzuordnen ist, gilt zum 1. April des Kalenderjahres, das auf das Kalenderjahr folgt, in dem ihr Versorgungsgrad den in Teil 3 Spalte D genannten Schwellenwert erstmalig erreicht oder überschreitet, als Kritische Infrastruktur. Hat der Versorgungsgrad einer Anlage den in Teil 3 Spalte D genannten Schwellenwert im Kalenderjahr 2015 erreicht oder überschritten, gilt die Anlage mit Inkrafttreten dieser Verordnung als Kritische Infrastruktur.

2.
Der Betreiber hat den Versorgungsgrad seiner Anlage für das zurückliegende Kalenderjahr bis zum 31. März des Folgejahres zu ermitteln.

3.
Stehen mehrere Anlagen derselben Art in einem engen räumlichen und betrieblichen Zusammenhang (gemeinsame Anlage) und erreichen oder überschreiten die in Teil 3 Spalte D genannten Schwellenwerte zusammen, gilt die gemeinsame Anlage als Kritische Infrastruktur. Ein enger räumlicher und betrieblicher Zusammenhang ist gegeben, wenn die Anlagen

a)
auf demselben Betriebsgelände liegen,

b)
mit gemeinsamen Betriebseinrichtungen verbunden sind,

c)
einem vergleichbaren technischen Zweck dienen und

d)
unter gemeinsamer Leitung stehen.

4.
Die Ermittlung des Versorgungsgrads kann mittels einer pauschalierten Umrechnung der in Teil 3 Spalte D genannten Schwellenwerte auf den in einem Kalenderjahr erzielten Bruttoumsatz in einem Verhältnis von 3,90 Euro pro kg oder l erfolgen.

Teil 2
Berechnungsformeln zur Ermittlung der Schwellenwerte

5.
Der für die Anlagenkategorien des Teils 3 genannte Schwellenwert (Speisen) ist unter Annahme einer durchschnittlichen Produktionsmenge zur Versorgung einer Person mit Lebensmitteln (Speisen) aller Produktgruppen von 0,869 Tonnen/Jahr sowie eines Regelschwellenwertes von 500 000 versorgten Personen wie folgt berechnet:

434 500 t/Jahr = 0,869 t/Jahr x 500 000

6.
Der für die Anlagenkategorien des Teils 3 genannte Schwellenwert (Getränke) ist unter Annahme eines Durchschnittsverbrauchs von 700 l/Jahr von nichtalkoholischen Getränken sowie eines Regelschwellenwertes von 500 000 versorgten Personen wie folgt berechnet:

350 Millionen l/Jahr = 700 l/Jahr x 500 000

Teil 3
Anlagenkategorien und Schwellenwerte

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Anlagenkategorie	Bemessungskriterium	Schwellenwert
1.	**Lebensmittelversorgung**		
1.1	Lebensmittelproduktion und -verarbeitung		
1.1.1	Anlage zur Produktion von Lebensmitteln	Menge der gewonnenen Lebensmittel in t/Jahr oder l/Jahr	Speisen: 434 500 t oder Getränke: 350 Millionen l
1.1.2	Anlage zur Bearbeitung und Verarbeitung von Lebensmitteln	Menge der bearbeiteten, verarbeiteten oder produzierten Lebensmittel oder Zwischenprodukte in t/Jahr oder l/Jahr	Speisen: 434 500 t oder Getränke: 350 Millionen l
1.1.3	Anlage zur Lagerung von Lebensmitteln	Menge der umgeschlagenen Lebensmittel in t/Jahr oder l/Jahr	Speisen: 434 500 t oder Getränke: 350 Millionen l
1.1.4	Anlage zur Distribution von Lebensmitteln	Menge der umgeschlagenen Lebensmittel in t/Jahr oder l/Jahr	Speisen: 434 500 t oder Getränke: 350 Millionen l
1.2.	Lebensmittelhandel		
1.2.1	Anlage zur Lagerung von	Menge der umgeschlagenen Lebensmittel	Speisen:

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Anlagenkategorie	Bemessungskriterium	Schwellenwert
	Lebensmitteln	in t/Jahr oder l/Jahr	434 500 t oder Getränke: 350 Millionen l
1.2.2	Anlage zur Distribution von Lebensmitteln	Menge der umgeschlagenen Lebensmittel in t/Jahr oder l/Jahr	Speisen: 434 500 t oder Getränke: 350 Millionen l
1.2.3	Anlage zur Bestellung von Lebensmitteln	Menge der bestellten Lebensmittel in t/Jahr oder l/Jahr	Speisen: 434 500 t oder Getränke: 350 Millionen l
1.2.4	Anlage zum Verkauf von Lebensmitteln	Menge der verkauften Lebensmittel in t/Jahr oder l/Jahr	Speisen: 434 500 t oder Getränke: 350 Millionen l

Anhang 4 (zu § 1 Nummer 4 und 5, § 5 Absatz 4 Nummer 1 und 2) Anlagenkategorien und Schwellenwerte im Sektor Informationstechnik und Telekommunikation
(Fundstelle: BGBl. I 2016,967 - 969)

Teil 1
Grundsätze und Fristen
1.
Für die in Teil 3 Spalte B genannten Anlagenkategorien gelten vorrangig die Begriffsbestimmungen nach § 3 des Telekommunikationsgesetzes in der jeweils geltenden Fassung.
2.
Eine Anlage, die einer in Teil 3 Spalte B genannten Anlagenkategorie zuzuordnen ist, gilt zum 1. April des Kalenderjahres, das auf das Kalenderjahr folgt, in dem ihr Versorgungsgrad den in Teil 3 Spalte D genannten Schwellenwert erstmals erreicht oder überschreitet, als Kritische Infrastruktur. Hat der Versorgungsgrad einer Anlage den in Teil 3 Spalte D genannten Schwellenwert im Kalenderjahr 2015 erreicht oder überschritten, gilt die Anlage mit Inkrafttreten dieser Verordnung als Kritische Infrastruktur.
3.
Der Betreiber hat den Versorgungsgrad seiner Anlage für das zurückliegende Kalenderjahr bis zum 31. März des Folgejahres zu ermitteln.
4.
Ist der Versorgungsgrad für die Anlagenkategorien des Teils 3 Nummer 1.1.1 bis 1.2.1 unmittelbar anhand der Anzahl versorgter Personen zu ermitteln, ist der Versorgungsgrad zum 30. Juni des zurückliegenden Kalenderjahres maßgeblich.
5.
Ist der Versorgungsgrad der genannten Anlagenkategorie anhand der Kapazität (installierte Leistung) einer Anlage zu ermitteln, ist auf den rechtlich und tatsächlich möglichen Betriebsumfang der durch denselben Betreiber betriebenen Anlage abzustellen.
6.
Stehen mehrere Anlagen derselben Art in einem engen betrieblichen Zusammenhang (gemeinsame Anlage) und erreichen oder überschreiten die in Teil 3 Spalte D genannten Schwellenwerte zusammen, gilt die gemeinsame Anlage als Kritische Infrastruktur. Ein enger betrieblicher Zusammenhang ist unabhängig von der räumlichen Distanz der Anlagen gegeben, wenn die Anlagen
a)
auf demselben Betriebsgelände liegen,
b)
mit gemeinsamen Betriebseinrichtungen oder untereinander verbunden sind,
c)
einem vergleichbaren technischen Zweck dienen und
d)
unter gemeinsamer Leitung oder Steuerung stehen.
Teil 2
Berechnungsformeln zur Ermittlung der Schwellenwerte
7.
Der für die Anlagenkategorien des Teils 3 Nummer 1.1 bis 1.2 genannte Schwellenwert ergibt sich aus § 1 Absatz 1 Nummer 2 des Post- und Telekommunikationssicherstellungsgesetzes vom 24. März 2011 (BGBl. I S. 506, 941) in der jeweils geltenden Fassung.

8.
Der für die Anlagenkategorie des Teils 3 Nummer 1.3.1 genannte Schwellenwert ist unter Annahme einer Anzahl von 50 000 Autonomen Systemen aus allen Netzen und einer Bedarfsabdeckung von 500 000 versorgten Personen bei einer Gesamtbevölkerung von 80 Millionen Personen wie folgt berechnet:

$$300 \approx \frac{500\,000}{80\,000\,000} \times 50\,000$$

9.
Der für die Anlagenkategorie des Teils 3 Nummer 1.4.1 genannte Schwellenwert ist unter Annahme der Benutzung von 5 IP-Endgeräten durch eine Person und eines Regelschwellenwertes von 500 000 versorgten Personen wie folgt berechnet:

$$2\,500\,000 = 5 \times 500\,000$$

10.
Der für die Anlagenkategorie des Teils 3 Nummer 1.4.2 genannte Schwellenwert ist unter Annahme von 40 Millionen in der Bundesrepublik Deutschland verwalteten Domains und einer Bedarfsabdeckung von 500 000 versorgten Personen bei einer Gesamtbevölkerung von 80 Millionen Personen wie folgt berechnet:

$$250\,000 \approx \frac{500\,000}{80\,000\,000} \times 40\,000\,000$$

11.
Der für die Anlagenkategorie des Teils 3 Nummer 2.2.1 genannte Schwellenwert ist unter Annahme von 4 Millionen in der Bundesrepublik Deutschland verwalteten Servern und einer Bedarfsabdeckung von 500 000 versorgten Personen bei einer Gesamtbevölkerung von 80 Millionen Personen wie folgt berechnet:

$$25\,000 = \frac{500\,000}{80\,000\,000} \times 4\,000\,000$$

12.
Der für die Anlagenkategorie des Teils 3 Nummer 2.2.2 genannte Schwellenwert ist unter Annahme eines Transportvolumens von 11 826 000 Terabyte/Jahr und einer Bedarfsabdeckung von 500 000 versorgten Personen bei 80 Millionen Personen Gesamtbevölkerung wie folgt berechnet:

$$75\,000\ \text{TByte/Jahr} \approx \frac{500\,000}{80\,000\,000} \times 11\,826\,000\ \text{TByte/Jahr}$$

Teil 3
Anlagenkategorien und Schwellenwerte

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Anlagenkategorie	Bemessungskriterium	Schwellenwert
1.	**Sprach- und Datenübertragung**		
1.1	Zugang		
1.1.1	Ortsgebundene Zugangsnetze, über die Zugang zu einem öffentlichen Telefondienst, zu einem öffentlichen Datenübermittlungsdienst oder Internetzugangsdienst erfolgt	Teilnehmeranschlüsse des Zugangsnetzes (§ 3 Nummer 21 TKG in der jeweils geltenden Fassung)	100 000 (§ 1 Absatz 1 Nummer 2 PTSG in der jeweils geltenden Fassung)
1.2.	Übertragung		
1.2.1	Übertragungsnetze für öffentlich zugängliche Telefondienste und Datenübermittlungsdienste oder Internetzugangsdienste (ohne Nummer 1.1.1)	Teilnehmer des jeweiligen Dienstes	100 000 (§ 1 Absatz 1 Nummer 2 PTSG in der jeweils geltenden Fassung)
1.3	Vermittlung		
1.3.1	IXP für öffentlich zugängliche Telefondienste, Datenübermittlungsdienste oder Internetzugangsdienste	Anzahl angeschlossener autonomer Systeme (Jahresdurchschnitt)	300
1.4.	Steuerung		
1.4.1	DNS-Resolver, die zur Nutzung öffentlich zugänglicher Telefondienste, Datenübermittlungsdienste oder Internetzugangsdienste angeboten werden	Anzahl der abfragenden IP-Adressen pro Tag (Jahresdurchschnitt)	2 500 000

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Anlagenkategorie	Bemessungskriterium	Schwellenwert
1.4.2	Autoritative DNS-Server, die zur Nutzung öffentlich zugänglicher Telefondienste, Datenübermittlungsdienste oder Internetzugangsdienste angeboten werden	Anzahl der Domains, für die der Server autoritativ ist oder die aus der Zone delegiert werden	250 000
2.	**Datenspeicherung und -verarbeitung**		
2.1	Housing		
2.1.1	Rechenzentrum	vertraglich vereinbarte Leistung in MW (am 30. Juni eines Kalenderjahres)	5
2.2.	IT-Hosting		
2.2.1	Serverfarm	Anzahl der laufenden Instanzen (Jahresdurchschnitt)	25 000
2.2.2	Content Delivery Netzwerk	ausgeliefertes Datenvolumen (in TByte/Jahr)	75 000
2.3.	Vertrauensdienste		
2.3.1	Anlage zur Erbringung von Vertrauensdiensten	Anzahl der ausgegebenen qualifizierten Zertifikate oder	500 000
		Anzahl von Zertifikaten zur Authentifizierung öffentlich zugänglicher Server (Serverzertifikate, z. B. für Webserver, E-Mailserver, Cloudserver (z. B. TLS/SSL-Zertifikate))	10 000

.

4. КНР

网络安全法（草案二次审议稿）全文 浏览字号： 大 中 小 来源： 中国人大网 2016年05月04日 （Cybersecurity Law (Draft) (Second Reading Draft))

[неофициальный перевод на английскийъ (http://chinalawtranslate.com/cybersecurity2/?lang=en#_Toc455489576)

People's Republic of China Cybersecurity Law (draft)

(Second Deliberation Draft)

Chapter I: General Provisions

Article 1: This law is formulated so as to ensure network security, to preserve cyberspace sovereignty, national security and the societal public interest, to protect the lawful rights and interests of citizens, legal persons and other organizations, and to promote the healthy development of economic and social informatization.
Article 2: This law applies with respect to the construction, operation, maintenance and usage of networks, as well as network security supervision and management within the mainland territory of the People's Republic of China.
Article 3: The State persists in equally stressing network security and informatization development, and abides by the directives of active use, scientific development, management in accordance with law, and ensuring security; and advances the construction of network infrastructure, encouraging innovation and application of network technology, establishing and completing systems to safeguard network security, and raising the capacity to protect network security.
Article 4: The State formulates and continuously improves a network security strategy, clarifies the fundamental requirements and primary goals of network security, and puts forward network security policies, work tasks, and procedures for key fields.
Article 5: The State takes measures for monitoring, preventing, and handling network security risks and threats arising both within and without the mainland territory of the People's Republic of China, protects critical information infrastructure against attacks, intrusions, interference and destruction; and punishes unlawful and criminal network activities in accordance with law, preserving cyberspace security and order.
Article 6: The State advocates sincere, honest, healthy and civilized network conduct; promoting dissemination of the core socialist values, adopting measures to raise the entire society's awareness and level of network security, and forming a good environment for the entire society to jointly participate in advancing network security.
Article 7: The State actively carries out international exchange and cooperation in the areas of cyberspace governance, research and development of network technologies, formulation of standards, attacking cybercrime and illegality, and other such areas; promoting the construction of a peaceful, secure, open and cooperative cyberspace; and establishing a network governance system that is multilateral, democratic and transparent.
Article 8: The State network information departments are responsible for comprehensively planning and coordinating network security efforts and related supervision and management efforts. The State Council Departments for telecommunications, public security, and other relevant organs, are responsible for network security protection, supervision and management

efforts within the scope of their responsibilities, in accordance with the provisions of this Law, relevant laws and administrative regulations.
Network security protection, supervision and management duties for relevant departments in people's governments at the county level or above will be determined by relevant national regulations.
Article 9: Network operators carrying out business and service activities must follow the laws and administrative regulations, follow social mores and commercial ethics, be honest and credible, perform obligations to protect network security, accept supervision from the government and public, and bear social responsibility.
Article 10: The construction and operation of networks, or the provision of services through networks, shall be in accordance with the provisions of laws and administrative regulations, and with the mandatory requirements of State standards; adopting technical measures and other necessary measures to safeguard network security and operational stability, effectively responding to network security incidents, preventing cybercrimes, and unlawful activity, and preserving the integrity, secrecy and usability of online data.
Article 11: Relevant network industry organizations are to, according to their Articles of Association, strengthen industry self-discipline, formulate behavioral network security norms, guide their members in strengthening network security protection according to the law, raise the protection levels of network security, and stimulate the healthy development of the industry.
Article 12: The State protects the rights of citizens, legal persons, and other organizations to use networks in accordance with law; it promotes widespread network access, raises the level of network services, it provides secure and convenient network services to society, and guarantees the lawful, orderly and free circulation of network information.
Any person and organization using networks shall abide by the Constitution and laws, observe public order and respect social morality; they must not endanger network security, and must not use the network to engage in activities endangering national security, inciting subversion of national sovereignty and the overturn of the socialist system, advocating terrorism and extremism, inciting ethnic hatred and ethnic discrimination, disseminating violent, obscene or sexual information, creating or disseminating false information to disrupt the economic or social order, as well as infringing on the reputation, privacy, intellectual property or other lawful rights and interests of others, and other such acts.
Article 13: All individuals and organizations have the right to report conduct endangering network security to departments such as for network information, telecommunications and public security. Departments receiving reports shall promptly process them in accordance with law; where these do not fall within the responsibilities of that department, they shall promptly transfer the matters to the department empowered to handle them.
Chapter II: Support And Advancement Of Network Security
Article 14: The State establishes and improves a system of network security standards. The State Council administrative department for standardization and other relevant State Council departments, on the basis of their individual responsibilities, organize the formulation and timely revision of relevant national and industry standards for network security management as well as for the security of network products, services and operations.
The State supports enterprises, network-related industry organizations, and so forth to participate in the formulation of national and industry standards for network security, and encourages enterprises to formulate enterprise standards that are stricter than the national or industry standards.
Article 15: The State Council and people's governments of provinces, autonomous regions and directly-governed municipalities shall make comprehensively plans; expand their input; support key network security technology industries and programs; support network security

technology research and development, application and popularization; spread safe and trustworthy network products and services; protect the intellectual property rights for network technologies; and support research and development institutions, higher education institutions, and so forth to participate in State network security technology innovation programs.

Article 16: The State advances the establishment of socialized service systems for network security, encouraging relevant enterprises and institutions to carry out network security certifications, testing, risk assessment and other such security services.

Article 17: The State encourages the development of network data security protections and utilization technologies, advancing the opening of public data resources, and promoting technological innovation, and economic and social development.

The State supports innovative methods of network security management, utilizing new network technologies to enhance the level of network security protections.

Article 18: All levels' of people's governments and their relevant departments shall organize and carry out regular network security publicity and education, and guide and stimulate relevant units in doing network security publicity and education work well.

The mass media shall conduct targeted network security publicity and education aimed at the public.

Article 19: The State supports enterprises, and education or training institutions such as higher learning institutions and vocational schools, in carrying out network security-related education and training, and employs multiple methods to cultivate talent in network security, and promote interaction of network security professionals.

Chapter III: Network Operations Security

Section 1: General Provisions

Article 20: The State implements a tiered network security protection system. Network operators shall perform the following security protection duties according to the requirements of the tiered network security protection system to ensure the network avoids interference, damage or unauthorized visits, and to prevent network data leaks, theft or falsification:

(1) Formulate internal security management systems and operating rules, determine persons responsible for network security, and implement network security protection responsibility;

(2) Adopt technological measures to prevent computer viruses, network attacks, network intrusions and other actions endangering network security;

(3) Adopt technological measures for monitoring and recording network operational statuses and network security incidents, and store network logs for at least six months;

(4) Adopt measures such as data classification, back-up of important data, and encryption;

(5) Other obligations provided by law or administrative regulations.

Article 21: Network products and services shall comply with the relevant national and mandatory requirements. Providers of network products and services must not install malicious programs; when discovering that their products and services have security flaws or vulnerabilities, they shall promptly inform users, adopt remedial measures, and follow provisions to report to the competent departments.

Providers of network products and services shall provide security maintenance for their products and services; and must not terminate providing security maintenance during the set time period or period agreed on with clients.

Where network products or services have functions collecting user information, their providers shall express this to users and obtain their consent; where citizens' personal information is collected, they shall obey the provisions of this law and other relevant laws and administrative regulations on protection of citizens' personal information.

Article 22: Critical network equipment and specialized network security products shall follow the national standards and mandatory requirements, and be safety certified by a qualified establishment or meet the requirements of a safety inspection, before being sold. The state network information departments, together with the relevant departments of the State Council, formulate and release a catalog of critical network equipment and specialized network security products, and promote reciprocal recognition of safety certifications and security inspection results to avoid duplicative certifications and inspections.

Article 23: Network operators handling network access and domain registration services for users, handling stationary or mobile phone network access, or providing users with information publication or instant messaging services, shall require users to provide real identity information when signing agreements with users or confirming provision of services. Where users do not provide real identity information, network operators must not provide them with relevant services.

The State implements a network identity credibility strategy, and supports research and development of secure and convenient electronic identity confirmation technologies, promoting reciprocal acceptance among different electronic identity confirmations.

Article 24: Network operators shall formulate emergency response plans for network security incidents, promptly addressing system vulnerabilities, computer viruses,network attacks, network incursions, and other such network security risks; and when network security incidents occur, immediately initiate the emergency response plan, adopt corresponding remedial measures, and report to the relevant competent departments in accordance with relevant provisions.

Article 25: Those carrying out network security certification, testing, risk assessment or other such activities, and publicly publishing network security information such as system vulnerabilities, computer viruses, network attacks, or network incursions, shall comply with relevant national provisions.

Article 26: Individuals and organizations must not engage in illegal entry of others' networks, disruption of the normal function of others' networks, theft of network data or other activities endangering network security; must not provide programs, or tools specially used in network incursions, disrupting normal network functions and protection measures, stealing network data or other acts endangering network security; and where clearly knowing that others will engage in actions endangering network security, must not provide them with help such as technological support, advertisements and promotion, or paying expenses.

Article 27: Network operators shall provide technical support and assistance to public security organs' and state security organs; lawful activities preserving national security and investigating crimes.

Article 28: The State supports cooperation between network operators in areas such as gathering, analyzing, reporting and responding to network security information, increasing the security safeguard capacity of network operators.

Relevant industry organizations are to establish and complete mechanisms for regulation and coordination of network security for their industry, strengthen their analysis and assessment of network security, and periodically conduct risk warnings for members, and shall support and coordinate members' responses to network security risks.

Section 2: Operations Security For Critical Information Infrastructure

Article 29: The State implements key protection of critical information infrastructure that if destroyed, losing function or leaking data might seriously endanger national security, national welfare and the people's livelihood, or the public interest, on the basis of their tiered protection system. The State Council will formulate the specific scope and security protection measures for critical information infrastructure.

The State encourages operators of networks outside the critical information infrastructure to voluntarily participate in the critical information infrastructure protection system.

Article 30: In accordance with the duties and division of labor provided by the State Council, departments responsible for security protection work of critical information infrastructure, are to separately compile and organize implementation of security plans for that industry or field's critical information infrastructure, and guide and supervise security protection efforts for the critical information infrastructure operations.

Article 31: Construction of critical information infrastructure shall ensure that it has properties for supporting business stability and sustaining operations, and ensures that technical security measures are planned, established and used concurrently.

Article 32: Except as provided in article 20 of this Law, critical information infrastructure operators shall also perform the following security protection duties:

(1) Set up specialized security management bodies and persons responsible for security management, and conduct security background checks on those responsible persons and personnel in critical positions;

(2) Periodically conduct network security education, technical training and skills evaluations for employees;

(3) Conduct disaster recovery backups of important systems and databases;

(4) Formulate emergency response plans for network security incidents, and periodically organize drills;

(5) Other obligations provided by law or administrative regulations.

Article 33: Critical information infrastructure information infrastructure operators purchasing network products and services that might impact national security shall go through a national security review organized by the State network information departments and relevant departments of the State Council.

Article 34: Critical information infrastructure operators purchasing network products and services shall sign a security and confidentiality agreement with the provider, clarifying duties and responsibilities for security and confidentiality.

Article 35: Citizens' personal information and other important business data gathered or produced by critical information infrastructure operators during operations within the mainland territory of the People's Republic of China, shall store it within mainland China. Where due to business requirements it is truly necessary to provide it outside the mainland, they shall follow the measures jointly formulated by the State network information departments and the relevant departments of the State Council to conduct a security assessment; but where laws and administrative regulations provide otherwise, follow those provisions.

Article 36: At least once a year, critical information infrastructure operators shall conduct an inspection and assessment of their networks security and risks that might exists either personally, or through retaining a network security services establishment; and submit a network security report on the circumstances of the inspection and assessment as well as improvement measures, to be sent to the relevant department responsible for critical information infrastructure security protection efforts.

Article 37: State network information departments shall coordinate relevant departments in employing the following measures for critical information infrastructure security protection:

(1) Conduct spot testing of critical information infrastructure security risks, put forward improvement measures, and when necessary may retain a network security service establishment to conduct testing and assessment of network security risks;

(2) Periodically organize critical information infrastructure operators to conduct emergency network security response drills, increasing the level, coordination, and capacity of responses to network security incidents.

(3) Advance network security information sharing among relevant departments, critical information infrastructure operators, and also research institutions, network security services establishments.
(4) Provide technical support and assistance for network security emergency management and recovery and so forth.
Article 38: Information obtained by State network information departments and relevant departments during critical information infrastructure protection can only be used as necessary for the protection of network security, and must not be used in other ways.
Chapter IV: Network Information Security
Article 39: Network operators shall establish and complete user information protection systems, and must strictly protect user information they collect.
Article 40: Network operators collecting and using citizens' personal information shall abide by the principles of legality, propriety and necessity; explicitly stating the purposes, means, and scope for collecting or using information, and obtaining the consent of the person whose data is gathered.
Network operators must not gather citizens' personal information unrelated to the services they provide; must not violate the provisions of laws, administrative regulations or agreements between the parties to gather or use citizens' personal information; and shall follow the provisions of laws, administrative regulations or agreements with users to process citizens' personal information they have stored.
Network operators collecting or using citizens' personal information shall disclose their rules for its collection and use.
Article 41: Network operators must not disclose, tamper with, or destroy citizens' personal information they gather; and, absent the consent of the person whose information was collected, must not provide citizens' personal information to others. Except, however, where it has been processed so that the specific individual is unidentifiable and cannot be recovered.
Network operators shall adopt technological measures and other necessary measures to ensure the security of citizens' personal information, and prevent citizens' personal information it gathers from leaking, being destroyed or lost. When the leak, destruction or loss of citizens' personal information occur, or might occur, remedial measures shall be immediately taken, users who might be affected shall be informed, and reports shall be made to the competent departments in accordance with regulations.
Article 42: Where citizens discover that network operators have violated the provisions of laws, administrative regulations or agreements between the parties to gather or use their personal information, they have the right to request the network operators delete their personal information; where discovering that personal information gathered or stored by network operators has errors, they have the right to request the network operators make corrections.
Article 43: Individuals or organizations must not steal or use other illegal methods to acquire citizens' personal information, and must not unlawfully sell or unlawfully provide others with citizens' personal information.
Article 44: Departments lawfully having network security supervision and management duties, and their staffs, must keep citizens' personal information, private information and commercial secrets, which they learn of in performing their duties, strictly confidential, and must not leak, sell, or unlawfully provide it to others.
Article 45: Network operators shall strengthen management of information published by users, and upon discovering information that the law or administrative regulations prohibits the publication or transmission of, they shall immediately stop transmission of that information, employ handling measures such as deleting it, to prevent the information from spreading, save relevant records, and report it to the relevant competent departments.

Article 46: Electronic information sent, or application software provided, by any individual or organization must not install malicious programs, and must not contain information that laws and administrative regulations prohibit the publication or transmission of.

Electronic information distribution service providers, and application software download service providers, shall perform security management duties; and where discovering that their users have conduct provided for in the preceding paragraph, shall stop providing services and employ measures such as removal, store relevant records and report to the relevant competent departments.

Article 47: Network operators shall establish network information security complaint and reporting systems, publicly disclose information such as the methods for making complaints or reports, and promptly accept and handle complaints and reports relevant to network information security.

Network operators shall cooperate with network information departments and relevant departments lawful implementation of supervision and inspections.

Article 48: The State network information departments and relevant departments perform network information security supervision and management responsibilities in accordance with law; and where discovering information the release or transmission of which is prohibited by laws or administrative regulations, shall request the network operators stop transmission, employ disposition measures such as deletion, and store relevant records; for information described above that comes from outside mainland People's Republic of China, they shall notify the relevant organization to adopt technological measures and other necessary measures to block transmission.

Chapter V: Monitoring, Early Warnings, And Emergency Responses

Article 49: The State establishes systems for network security monitoring, early warnings and information bulletins. The State network information departments shall do overall coordination of relevant departments to strengthen collection, analysis and reporting efforts for network security information, and follow regulations for the unified release of network security monitoring and early warning information.

Article 50: Departments responsible for critical information infrastructure security protection efforts shall establish and complete that industry or that field's network security monitoring, early warning and information reporting systems, and report network security monitoring and early warning information in accordance with regulations.

Article 51: The State network information departments coordinates relevant departments' establishment and completion of mechanisms for network security risk assessment and emergency response efforts, formulates network security incident emergency response plans, and periodically organizes drills.

Departments responsible for critical information infrastructure security protection efforts shall formulate that industry or that field's network security incident emergency response plans, and periodically organize drills.

Network security incident emergency response plans shall rank network security incidents on the basis of factors such as the degree of threat after the incident occurs and the scope of impact, and provide corresponding emergency response handling measures.

Article 52: When the risk of network security incidents increases, the relevant departments of people's governments at the provincial level and above shall follow the scope of authority and procedures provided, and employ the following measures on the basis of the network security risk's characteristics and the harms it might cause:

(1) Require that relevant departments, institutions and personnel promptly gather and report relevant information, and strengthen monitoring of the occurrence of network security risks;

(2) Organize relevant departments, institutions and specialist personnel to conduct analysis and assessment of information on the network security risk, and predict the likelihood of an incident's occurrence, the scope of its impact and its level of harm;
(3) Publish network security risk warnings to the public, and publish measures for avoiding or reducing harms.

Article 53: On occurrence of a network security incident, the network security incident emergency response plan shall be immediately initiated, an evaluation and assessment of the network security incident shall be conducted, network operators shall be requested to adopt technological and other necessary measures, potential security risks shall be removed, the threat shall be prevented from growing, and warnings relevant to the public shall be promptly published.

Article 54: Where, while performing network security supervision and management duties, relevant departments of people's governments at the provincial level or above discover that networks have a relatively large security risk or the occurrence of a security incident, they may call in the legal representative or responsible party for the operator of that network for a talking to, in accordance with the scope of authority and procedures provided. Network operators shall follow requirements to employ procedures, make corrections, and eliminate hidden dangers.

Article 55: Where sudden emergencies or production safety accidents occur as a result of network security incidents, they shall be handled in accordance with the provisions the "Emergency Response Law of the People's Republic of China" , the "Production Safety Law of the People's Republic of China", and other relevant laws and administrative regulations.

Article 56: To fulfill the need to protect national security and social public order, and respond to major social security incidents, the State Council, or the governments of provinces, autonomous regions and municipalities with approval by the State Council, may take temporary measures regarding network communications in certain regions, such as restricting it.

Chapter VI: Legal Responsibility

Article 57: Where network operators do not perform network security protection duties provided for in articles 20 and 24 of this law, the competent departments will order corrections and give warnings; where corrections are refused or it leads to endangerment of network security or other such consequences, a fine of between RMB 10,000 and 100,000 is given; and the directly responsible management personnel are fined between RMB 5,000 and 50,000.

Where critical information infrastructure operators do not perform network security protection duties provided for in articles 31-34 and 36 of this law, the competent departments will order corrections and give warnings; where corrections are refused or it leads to endangerment of network security or other such consequences, a fine of between RMB 100,000 and 1,000,000 is give; and the directly responsible management personnel is fined between RMB 10,000 and 100,000.

Article 58: Where paragraphs 1 or 2 of article 21, or paragraph 1 of article 46 of this law are violated by any of the following conduct, the relevant competent departments order corrections and give warnings; where corrections are refused or it causes endangerment of network security or other consequences, a fine of between RMB 50,000 and 500,000 is given; and the persons who are directly in charge are fined between RMB 10,000 and 100,000.

(1) Installing malicious programs;
(2) Failure to promptly inform users and to take remedial measures for security flaws or vulnerabilities that exist in products or services, or not reporting this to the competent departments in accordance with provisions;

(3) Unauthorized ending of the provision of security maintenance for their products or services.

Article 59: Network operators violating paragraph 1 of articles 23 of this law in failing to require users to provide truthful identity information or providing relevant services to users who do not provide truthful identity information, are ordered to make corrections by the relevant competent department; where corrections are refused or the circumstances are serious, a fine of between RMB 50,000 and 500,000 is given, and the relevant competent department may order a temporary suspension of operations, a suspension of business for corrections, closing down of websites, cancellation of relevant operations permits, or cancellation of business licenses; persons who are directly in charge and other directly responsible personnel are fined between RMB 10,000 and 100,000.

Article 60: Where Article 25 of this law is violated in carrying out network security certifications, testing or risk assessments, or publishing network security information such as system vulnerabilities, computer viruses, network attacks, or network incursions, corrections are to be ordered and a warning given; where corrections are refused or the circumstances are serious, a fine of between RMB 10,000 and 100,000 is given, and the relevant competent department may order a temporary suspension of operations, a suspension of business for corrections, closing down of websites, cancellation of relevant operations permits, or cancellation of business licenses; persons who are directly in charge and other directly responsible personnel are fined between RMB 5,000 and 50,000.

Article 61: Where Article 26 of this law is violated in engaging in activities endangering national security, or by providing specialized software or tools used in engaging in activities endangering national security, or by providing others engaging in activities endangering network security with assistance such as technical support, advertising and promotions or payment of expenses; and a crime is no constituted, the public security organs are to confiscate unlawful gains and impose up to 5 days detention, and may give a fine of between 10,000 and 15,000 RMB; and where circumstances are serious, impose between 5 and 15 days detention, and may give a fine of between 50,000 and 500,000 RMB.

Where units exhibit the conduct provided for in the preceding paragraph, the public security organs confiscate unlawful gains, and impose a fine of between 100,000 and 500,000 RMB, and the directly responsible managers and other responsible personnel are punished in accordance with the preceding paragraph.

Where Article 26 of this law is violated, persons who receive public security administrative sanctions or criminal punishments must not take on work in key network security management and network operations positions for their lifetimes.

Article 62: Network operators, and network product or service providers, violating paragraph 3 of article 21 and Articles 40-42 of this Law by infringing on citizens' personal information that are protected in accordance with law, are ordered to make corrections by the relevant competent department and may, either independently or concurrently, be given warnings, confiscation of unlawful gains, and/or fined between 1 to 10 times the amount of unlawful gains, and where there are no unlawful gains, fined up to RMB 500,000; where the circumstances are serious, a fine of between RMB 50,000 and 500,000 is given, and the relevant competent department may order a temporary suspension of operations, a suspension of business for corrections, closing down of websites, cancellation of relevant operations permits, or cancellation of business licenses; persons who are directly in charge and other directly responsible personnel are fined between RMB 10,000 and 100,000.

Where violations of this law in stealing or using other illegal means to obtain, sell of illegally provide others with citizens' personal information do not constitute a crime, the public security organs confiscate unlawful gains and give a fine of between 1 and 10 times the

amount of unlawful gains, and where there are no unlawful gains, give a fine of up to RMB 500,000.

Article 63: Where critical information infrastructure operators violate article 33 of this Law by using network products or services that have not had safety inspections or did not pass safety inspections, the relevant competent departments order the usage to stop, and give a fine in the amount of 1 to 10 times the purchase price; the persons who are directly in charge and other directly responsible personnel are fined between RMB 10,000 and 100,000.

Article 64: Where critical information infrastructure operators violate this law by storing network data outside the mainland territory, or provide network data to individuals or organizations outside of the mainland territory without going through a security assessment, the relevant competent department orders corrections, gives warnings, confiscates unlawful gains, gives fines between RMB 50,000 and 500,000, and may order a temporary suspension of operations, a suspension of business for corrections, closing down of websites, revocation of relevant operations permits, or cancellation of business licenses; persons who are directly in charge and other directly responsible personnel are fined between RMB 10,000 and 100,000.

Article 65: Where network operators violate Article 45 of this Law by failing to stop the transmission of information that laws of administrative regulations prohibit the publication or transmission of, failing to employ disposition measures such as deletion or failure to preserve relevant records, the relevant competent department orders corrections, gives warnings, and confiscates unlawful gains; where corrections are refused or circumstances are serious, fines between RMB 50,000 and 500,000 are given, and a temporary suspension of operations, a suspension of business for corrections, closing down of websites, cancellation of relevant operations permits, or cancellation of business licenses may be ordered; persons who are directly in charge and other directly responsible personnel are fined between RMB 10,000 and 100,000.

Where electronic information service providers and application software download service providers, have not performed their security management duties provided for in paragraph 2 of Article 46 of this Law, punishment is in accordance with the provisions of the preceding paragraph.

Article 66: Network operators violating the provisions of this law, who exhibit any of the following conduct, will be ordered to make corrections by the relevant competent departments; where corrections are refused or the circumstances are serious, a fine of between 50,000 and RMB 500,000 is given; directly responsible management personnel and other directly responsible personnel are to be fined between RMB 10,000 and RMB 100,000:

(1) Failure to report network security risks or network security incidents to the relevant competent departments;

(2) Not following the requirements of relevant departments to adopt disposition measures such as stopping dissemination or deleting information that laws or administrative regulations prohibit the public or dissemination of;

(3) Refusal or obstruction of the relevant departments in their lawful conduct of supervision and inspections;

(4) Refusing to provide technical support and assistance to public security organs' and state security organs.

Article 67: Publication or transmission of information that paragraph 2 of Article 12 of this Law or other laws or administrative regulations prohibit the publication or transmission of, is punished in accordance with the provisions of the relevant laws and administrative regulations.

Article 68: Where there is conduct violating the provisions of this law, record it in the credit archives and make it public in accordance with relevant laws and administrative regulations.

Article 69: Where state organ government affairs network operators do not perform network security protection duties as provided by this law, the organ at the level above or relevant department will order corrections; sanctions are given to the directly responsible managers and other directly responsible personnel.

Article 70: Where personnel of departments bearing network safety supervision and management duties in accordance with law, neglect their duties, abuse their authority, or distort the law for personal gain, and it does not constitute a crime, sanctions are given in accordance with law.

Article 71: Where violations of the provisions of this law cause harm to others, civil liability is borne in accordance with law.

Where provisions of this Law are violated, constituting a violation of public security management, public security administrative sanctions are given in accordance with law; where a crime is constituted, criminal responsibility is pursued in accordance with law.

Chapter VII: Supplementary Provisions

Article 72: For this law, the following terms have these meanings:

(1) "Networks" refers to systems comprised of computers or other information terminals and related equipment that follow certain rules and procedures for information gathering, storage, transmission, exchange and processing.

(2) "Network security" refers to taking necessary measures to prevent network attacks, incursions, interference, destruction and their unlawful use, as well as unexpected accidents; to put the networks in a state of stable and reliable operation, as well as ensuring the capacity for network data to be complete, confidential and usable.

(3) "Network operators" refers to network owners, managersm and network service providers.

(4) "Network data" refers to all kinds of electronic data collected, stored, transmitted, processed, and produced through networks.

(5) "Citizens' personal information" refers to all kinds of information, recorded electronically or through other means, that taken alone or together with other information, is sufficient to identify a citizen's identity, including, but not limited to, citizens' full names, birth dates, identification numbers, personal biometric information, addresses, telephone numbers, and so forth.

Article 73: Operations security protections for storing and processing networks involving state secret information, shall follow this Law and shall also uphold laws and administrative regulations on secrecy.

Article 74: Security protections for military network are formulated by the Central Military Commission.

Article 75: This law shall take effect on XXXXX.

5. РФ

Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» (проект). Паспорт законопроекта

(https://regulation.gov.ru/projects?type=ListView#npa=597)

Проект
Экз № __

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНЫЙ ЗАКОН

О БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Глава 1. Общие положения

Статья 1. Сфера действия настоящего Федерального закона
Настоящий Федеральный закон устанавливает организационные и правовые основы обеспечения безопасности критической информационной инфраструктуры Российской Федерации в целях предотвращения компьютерных инцидентов, основные принципы и методы государственного регулирования в указанной сфере, порядок взаимодействия субъектов критической информационной инфраструктуры Российской Федерации с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, определяет полномочия органов государственной власти Российской Федерации, а также права, обязанности и ответственность субъектов критической информационной инфраструктуры Российской Федерации.
Статья 2. Основные понятия, используемые в настоящем Федеральном законе
Автоматизированная система управления производственными и технологическими процессами критически важного объекта инфраструктуры Российской Федерации – комплекс аппаратных и программных средств, информационных систем и информационно-телекоммуникационных сетей, предназначенных для решения задач оперативного управления и контроля за различными процессами и техническими объектами в рамках организации производства или технологического процесса критически важного объекта;
аккредитация – официальное признание федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации (далее – уполномоченные федеральные органы исполнительной власти) компетентности организации выполнять работы в области оценки защищенности критической информационной инфраструктуры Российской Федерации;
безопасность критической информационной инфраструктуры Российской Федерации – состояние объектов критической информационной инфраструктуры Российской Федерации и критической информационной инфраструктуры Российской Федерации в

целом, при котором возникновение на них компьютерных инцидентов не приведет к потере управления экономикой и/или обеспечения обороноспособности, безопасности и правопорядка Российской Федерации, субъекта Российской Федерации или административно-территориальной единицы, ее необратимому негативному изменению (разрушению) либо существенному снижению безопасности жизнедеятельности населения;

государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации – единая централизованная, территориально распределенная система, включающая силы и средства обнаружения и предупреждения компьютерных инцидентов, а также органы государственной власти, в полномочия которых входит обеспечение безопасности объектов критической информационной инфраструктуры Российской Федерации;

информационные ресурсы Российской Федерации – информационные системы и информационно-телекоммуникационные сети, находящиеся на территории Российской Федерации и в дипломатических представительствах и консульских учреждениях Российской Федерации за рубежом;

компьютерная атака – целенаправленное воздействие на информационные ресурсы программно-техническими средствами, осуществляемое в целях нарушения безопасности информации в этих ресурсах;

компьютерный инцидент – факт нарушения (или прекращения) функционирования объекта критической информационной инфраструктуры Российской Федерации, в том числе вызванный компьютерной атакой;

критически важный объект – объект, нарушение или прекращение функционирования которого может привести к потере управления экономикой Российской Федерации, субъекта Российской Федерации или административно-территориальной единицы, ее необратимому негативному изменению (разрушению) либо существенному снижению безопасности жизнедеятельности населения;

критическая информационная инфраструктура Российской Федерации – совокупность автоматизированных систем управления производственными и технологическими процессами критически важных объектов и обеспечивающих их взаимодействие информационно-телекоммуникационных сетей, а также информационных систем и сетей связи, предназначенных для решения задач государственного управления, обеспечения обороноспособности, безопасности и правопорядка (далее – объекты критической информационной инфраструктуры Российской Федерации);

нарушение функционирования критической информационной инфраструктуры Российской Федерации – отрицательные последствия целенаправленного и/или случайного воздействия на объекты критической информационной инфраструктуры Российской Федерации, приведшие к утечке, хищению, утрате, подделке, искажению и несанкционированному доступу к информации, а также к отклонению от установленных эксплуатационных пределов и условий функционирования объектов критической информационной инфраструктуры Российской Федерации;

субъекты критической информационной инфраструктуры Российской Федерации – юридические лица, владеющие на праве собственности или ином законном основании объектами критической информационной инфраструктуры Российской Федерации, операторы связи, а также операторы государственных информационных систем, обеспечивающие функционирование и взаимодействие объектов критической информационной инфраструктуры Российской Федерации.

Статья 3. Законодательство о безопасности критической информационной инфраструктуры Российской Федерации

1. Законодательство Российской Федерации о безопасности критической информационной инфраструктуры Российской Федерации основывается на Конституции Российской Федерации и состоит из настоящего Федерального закона, других федеральных законов и принимаемых в соответствии с ними иных нормативных правовых актов Российской Федерации.
2. Если международным договором Российской Федерации установлены иные правила, чем те правила, которые предусмотрены настоящим Федеральным законом, применяются правила международного договора Российской Федерации.
Статья 4. Обеспечение безопасности критической информационной инфраструктуры Российской Федерации
1. Обеспечение безопасности критической информационной инфраструктуры Российской Федерации включает комплекс мер правового, организационного и технического характера по созданию и эксплуатации систем безопасности объектов критической информационной инфраструктуры Российской Федерации и их взаимодействию с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации в целях недопущения нарушения или прекращения функционирования критической информационной инфраструктуры Российской Федерации.
2. Основными направлениями обеспечения безопасности критической информационной инфраструктуры Российской Федерации являются:
1) нормативное правовое регулирование деятельности по обеспечению безопасности критической информационной инфраструктуры Российской Федерации;
2) определение уполномоченных федеральных органов исполнительной власти, осуществляющих мероприятия по обеспечению безопасности критической информационной инфраструктуры Российской Федерации;
3) разработка и реализация федеральных целевых программ обеспечения безопасности критической информационной инфраструктуры Российской Федерации;
4) установление обязательных требований по обеспечению безопасности объектов критической информационной инфраструктуры Российской Федерации, их технической защищенности, в том числе при создании, вводе в эксплуатацию, эксплуатации и модернизации (на всех этапах жизненного цикла);
5) категорирование объектов критической информационной инфраструктуры Российской Федерации;
6) оценка защищенности объектов критической информационной инфраструктуры Российской Федерации;
7) создание и обеспечение функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;
8) государственный контроль (надзор) в области безопасности критической информационной инфраструктуры Российской Федерации;
9) информационно-аналитическое, материально-техническое и научно-техническое обеспечение безопасности критической информационной инфраструктуры Российской Федерации;
10) выявление угроз безопасности критической информационной инфраструктуры Российской Федерации;
11) обнаружение, предупреждение и ликвидация последствий компьютерных атак на информационные ресурсы Российской Федерации.
3. Разработка мероприятий по обеспечению безопасности критической информационной инфраструктуры Российской Федерации осуществляется уполномоченными федеральными органами исполнительной власти и субъектами

критической информационной инфраструктуры Российской Федерации на основе проведенного категорирования объектов критической информационной инфраструктуры Российской Федерации в соответствии с требованиями настоящего Федерального закона и принятыми в соответствии с ним нормативными правовыми актами.

4. Уполномоченные федеральные органы исполнительной власти в пределах своей компетенции принимают участие в международном сотрудничестве в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, участвуют в работе международных организаций, совещаний и конференций по вопросам обеспечения безопасности критической информационной инфраструктуры Российской Федерации, а также в соответствии с международными договорами осуществляют обмен информацией на взаимной основе с органами иностранных государств и международными организациями о возможных угрозах безопасности и выявленных компьютерных инцидентах.

Глава 2. Государственная политика в сфере обеспечения безопасности критической информационной инфраструктуры Российской Федерации

Статья 5. Цель и принципы обеспечения безопасности критической информационной инфраструктуры Российской Федерации

1. Целью обеспечения безопасности критической информационной инфраструктуры Российской Федерации является ее устойчивое и безопасное функционирование, обеспечивающее защиту интересов личности, общества и государства в информационной сфере.

2. Основными принципами обеспечения безопасности критической информационной инфраструктуры Российской Федерации являются:

1) законность;

2) соблюдение баланса интересов личности, общества и государства;

3) взаимная ответственность личности, общества и государства в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации;

4) непрерывность и комплексность обеспечения безопасности критической информационной инфраструктуры Российской Федерации;

5) эффективное взаимодействие уполномоченных федеральных органов исполнительной власти и субъектов критической информационной инфраструктуры Российской Федерации;

6) приоритет предупреждения компьютерных инцидентов в критической информационной инфраструктуре Российской Федерации.

Статья 6. Полномочия органов государственной власти в сфере обеспечения безопасности критической информационной инфраструктуры Российской Федерации

1. Президент Российской Федерации:

1) определяет основные направления государственной политики в сфере обеспечения безопасности критической информационной инфраструктуры Российской Федерации;

2) определяет порядок создания и принципы построения государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;

3) определяет случаи использования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации для решения задач, не связанных с обеспечением безопасности объектов критической инфраструктуры Российской Федерации.

2. Правительство Российской Федерации

организует обеспечение федеральных органов исполнительной власти средствами и ресурсами, необходимыми для выполнения задач в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации.

3. Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности:

1) осуществляет реализацию государственной политики в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации;

2) осуществляет научно-исследовательскую деятельность в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации;

3) координирует деятельность субъектов критической информационной инфраструктуры Российской Федерации в области обнаружения, предупреждения и ликвидации компьютерных инцидентов;

4) по согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации вносит предложения о совершенствовании нормативного правового регулирования в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации Президенту Российской Федерации и в Правительство Российской Федерации;

5) проводит оценку защищенности объектов критической информационной инфраструктуры Российской Федерации для объектов критической информационной инфраструктуры Российской Федерации высокой категории опасности;

6) проводит проверку на достоверность и правильность отнесения объектов критической информационной инфраструктуры Российской Федерации к высокой категории опасности;

7) ведет реестр объектов критической информационной инфраструктуры Российской Федерации высокой категории опасности, утверждает форму указанного реестра и правила его ведения;

8) проводит аккредитацию организаций для осуществления ими деятельности по оценке защищенности объектов критической информационной инфраструктуры Российской Федерации высокой категории опасности;

9) осуществляет государственный контроль (надзор) в области обеспечения безопасности объектов критической информационной инфраструктуры Российской Федерации высокой категории опасности, а также устанавливает порядок его осуществления;

10) совместно с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации, разрабатывает и утверждает показатели критериев категорирования объектов критической информационной инфраструктуры Российской Федерации;

11) устанавливает по согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации, требования к обеспечению безопасности объектов критической информационной инфраструктуры Российской Федерации высокой категории опасности;

12) осуществляет иные предусмотренные настоящим Федеральным законом полномочия.

4. Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации:
1) осуществляет реализацию государственной политики в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации;
2) осуществляет научно-исследовательскую деятельность в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации;
3) по согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, вносит предложения о совершенствовании нормативного правового регулирования в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации Президенту Российской Федерации и в Правительство Российской Федерации;
4) проводит оценку защищенности объектов критической информационной инфраструктуры Российской Федерации для объектов критической информационной инфраструктуры Российской Федерации средней и низкой категорий опасности;
5) проводит проверку на достоверность и правильность отнесения объектов критической информационной инфраструктуры Российской Федерации к средней и низкой категориям опасности;
6) ведет реестр объектов критической информационной инфраструктуры Российской Федерации средней и низкой категорий опасности, утверждает форму указанного реестра и правила его ведения;
7) проводит аккредитацию организаций для осуществления ими деятельности по оценке защищенности объектов критической информационной инфраструктуры Российской Федерации средней и низкой категорий опасности;
8) осуществляет государственный контроль (надзор) в области обеспечения безопасности объектов критической информационной инфраструктуры Российской Федерации средней и низкой категорий опасности, а также устанавливает порядок его осуществления;
7) совместно с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности разрабатывает и утверждает показатели критериев категорирования объектов критической информационной инфраструктуры Российской Федерации;
8) устанавливает по согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, требования к обеспечению безопасности объектов критической информационной инфраструктуры Российской Федерации низкой и средней категории опасности;
9) осуществляет иные предусмотренные настоящим Федеральным законом полномочия.
Статья 7. Финансирование мероприятий по обеспечению безопасности критической информационной инфраструктуры Российской Федерации
1. Финансирование мероприятий по обеспечению безопасности критической информационной инфраструктуры Российской Федерации осуществляется за счет средств субъектов, которым объекты критической информационной инфраструктуры Российской Федерации принадлежат на праве собственности или ином законном основании, а также средств федерального бюджета, выделенных уполномоченным федеральным органам исполнительной власти на осуществление таких мероприятий.
2. Финансирование организации и функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных инцидентов

на информационные ресурсы Российской Федерации осуществляется за счет средств федерального бюджета.
3. Финансирование мероприятий по обеспечению безопасности объектов критической информационной инфраструктуры Российской Федерации за счет иных источников средств осуществляется в соответствии с законодательством Российской Федерации.

Глава 3. Обеспечение безопасности объектов критической информационной инфраструктуры Российской Федерации

Статья 8. Категорирование объектов критической информационной инфраструктуры Российской Федерации
1. Для установления дифференцированных требований обеспечения безопасности объектов критической информационной инфраструктуры Российской Федерации с учетом возможных последствий нарушения или прекращения их функционирования проводится категорирование объектов на основе критериев, установленных частью 2 настоящей статьи.
2. Категорирование объектов критической информационной инфраструктуры Российской Федерации осуществляется исходя из следующих критериев:
критерий экономической значимости;
критерий экологической значимости;
критерий значимости для обеспечения обороноспособности;
критерий значимости для национальной безопасности;
критерий социальной значимости;
критерий важности объекта критической информационной инфраструктуры Российской Федерации в части реализации управленческой функции;
критерий важности объекта критической информационной инфраструктуры Российской Федерации в части предоставления значительного объема информационных услуг.
3. С учетом указанных в части 2 настоящей статьи критериев устанавливаются следующие категории объектов критической информационной инфраструктуры Российской Федерации:
1) объекты критической информационной инфраструктуры Российской Федерации высокой категории опасности;
2) объекты критической информационной инфраструктуры Российской Федерации средней категории опасности;
3) объекты критической информационной инфраструктуры Российской Федерации низкой категории опасности.
4. Субъекты критической информационной инфраструктуры Российской Федерации на основании установленных частью 2 настоящей статьи критериев и в соответствии с утвержденными показателями этих критериев, осуществляют отнесение принадлежащих им на праве собственности или ином законном основании объектов критической информационной инфраструктуры Российской Федерации к установленным категориям.
5. Сведения о результатах проведенного категорирования субъекты критической информационной инфраструктуры Российской Федерации направляют:
- в отношении объектов высокой категории опасности – в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, по утвержденной им форме;
- в отношении объектов средней и низкой категории опасности - в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности

информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации, по утвержденной им форме.
6. Полученные сведения о результатах проведенного категорирования подлежат проверке на достоверность и правильность отнесения объекта критической информационной инфраструктуры Российской Федерации к определенной категории.
7. При несоответствии предоставленных сведений утвержденным показателям критериев либо при несоблюдении формы предоставления этих сведений уполномоченный федеральный орган исполнительной власти, возвращает субъекту критической информационной инфраструктуры Российской Федерации предоставленные им документы на доработку с мотивированным обоснованием причин возврата.
8. При соответствии предоставленных сведений утвержденным показателям критериев и форме предоставления этих сведений объекты критической информационной инфраструктуры Российской Федерации высокой категории опасности включаются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности в реестр объектов критической информационной инфраструктуры Российской Федерации высокой категории опасности, а объекты критической информационной инфраструктуры Российской Федерации средней и низкой категории опасности включаются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации, в реестр объектов критической информационной инфраструктуры Российской Федерации средней и низкой категории опасности.
9. Пересмотр категории объекта критической информационной инфраструктуры Российской Федерации может производиться в порядке категорирования, предусмотренном пунктами 4 – 6 настоящей статьи, по инициативе субъекта критической информационной инфраструктуры Российской Федерации или по обоснованному решению уполномоченного федерального органа исполнительной власти, в том числе по результатам проведенной оценки защищенности этого объекта.
Статья 9. Оценка защищенности критической информационной инфраструктуры Российской Федерации
1. Оценка защищенности критической информационной инфраструктуры Российской Федерации проводится на основе оценки защищенности ее объектов, анализа данных, получаемых при использовании технических средств государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, информации о признаках компьютерных атак в сетях электросвязи, а также иной информации, получаемой в соответствии с законодательством Российской Федерации.
2. В целях реализации части 1 настоящей статьи федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, устанавливает в сетях электросвязи технические средства, предназначенные для поиска признаков компьютерных атак в сообщениях электросвязи.
3. Технические условия, порядок установки и эксплуатации технических средств, указанных в частях 1 и 2 настоящей статьи, определяются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности.
4. Оценка защищенности объектов критической информационной инфраструктуры Российской Федерации проводится в целях определения состояния их защищенности, соответствующей определённой категории объектов критической информационной

инфраструктуры Российской Федерации, от потенциальных угроз возникновения компьютерных инцидентов.
5. Порядок проведения оценки защищенности Российской Федерации устанавливается:
- в отношении объектов критической информационной инфраструктуры Российской Федерации высокой категории опасности – федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности;
- в отношении объектов критической информационной инфраструктуры Российской Федерации средней и низкой категориям опасности – федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации.
7. При проведении оценки защищенности объектов критической информационной инфраструктуры Российской Федерации могут привлекаться аккредитованные для этих целей в установленном порядке организации.
8. На основе проведенной оценки защищенности объектов критической информационной инфраструктуры Российской Федерации уполномоченным федеральным органом исполнительной власти составляется акт, который содержит результаты проведенной оценки защищенности, а также, в необходимых случаях, предписание субъекту критической информационной инфраструктуры Российской Федерации в отношении мер, которые необходимо дополнительно включить в систему безопасности объекта критической информационной инфраструктуры Российской Федерации.
9. Сведения, полученные в ходе проведения оценки защищенности, раскрывающие уязвимость объекта критической информационной инфраструктуры Российской Федерации, относятся к информации ограниченного доступа. Если федеральным законом такие сведения отнесены к сведениям, составляющим государственную тайну, они подлежат защите в соответствии с законодательством Российской Федерации о государственной тайне.
Статья 10. Аккредитация организаций для осуществления ими деятельности по оценке защищенности объектов критической информационной инфраструктуры Российской Федерации
1. Аккредитация организаций для осуществления ими деятельности по оценке защищенности объектов критической информационной инфраструктуры Российской Федерации проводится на добровольной основе. Аккредитация организаций проводится на срок пять лет, если более короткий срок не указан в заявлении организации.
2. Аккредитация организаций проводится при условии выполнения ими следующих требований:
- наличие лицензии на проведение работ, связанных с использованием сведений, составляющих государственную тайну;
- наличие средств, предназначенных для оценки защищенности объектов критической информационной инфраструктуры Российской Федерации и получивших подтверждение соответствия требованиям, установленным в соответствии с частью 7 статьи 13 настоящего Федерального закона;
- наличие в штате организации не менее трех работников, непосредственно осуществляющих деятельность по оценке защищенности объектов критической информационной инфраструктуры Российской Федерации, имеющих высшее профессиональное образование в области информационной безопасности.
3. Аттестат аккредитации выдается на основании представленных заявителем заявления о предоставлении аттестата аккредитации и документов, подтверждающих

соответствие заявителя требованиям аккредитации. Исчерпывающий перечень таких документов содержится в порядке проведения аккредитации, установленном уполномоченным федеральным органом исполнительной власти.
4. Основанием отказа в предоставлении аттестата аккредитации является:
- наличие в представленных заявителем заявлении о предоставлении аттестата аккредитации и (или) прилагаемых к нему документах недостоверной или искаженной информации;
- установленное при проведении документарной проверки несоответствие заявителя требованиям аккредитации.
5. Основаниями для досрочного аннулирования аттестата аккредитации являются:
- обращение организации о прекращении деятельности по оценке защищенности объектов критической информационной инфраструктуры Российской Федерации;
- прекращение действия лицензии на осуществление работ, связанных с использованием сведений, составляющих государственную тайну, выданной организации.
6. Критерии аккредитации и порядок ее проведения устанавливаются:
- в отношении организаций для осуществления ими деятельности по оценке защищенности объектов критической информационной инфраструктуры Российской Федерации высокой категории опасности, – федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности;
- в отношении организаций для осуществления ими деятельности по оценке защищенности объектов критической информационной инфраструктуры Российской Федерации средней и низкой категорий опасности, – федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации.
Статья 11. Требования по обеспечению безопасности объекта критической информационной инфраструктуры Российской Федерации
1. Требования по обеспечению безопасности объекта критической информационной инфраструктуры Российской Федерации включают:
организационные вопросы безопасности;
требования к персоналу, непосредственно обеспечивающему функционирование и безопасность объектов критической информационной инфраструктуры Российской Федерации;
требования к защите от вредоносного программного обеспечения и от компьютерных атак;
требования безопасности при взаимодействии с сетями связи общего пользования;
требования к обеспечению безопасности информационных технологий в ходе эксплуатации информационно-телекоммуникационных систем.
2. Федеральные органы исполнительной власти, осуществляющие функции по выработке государственной политики и нормативно-правовому регулированию в установленной сфере деятельности, могут устанавливать дополнительные требования по обеспечению безопасности объектов критической информационной инфраструктуры Российской Федерации, исходя из специфики этих объектов, по согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, – в отношении объектов критической информационной инфраструктуры Российской Федерации высокой категории опасности или с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и

технической защиты информации, – в отношении объектов критической информационной инфраструктуры Российской Федерации средней и низкой категории опасности.

Статья 12. Права и обязанности субъектов критической информационной инфраструктуры Российской Федерации

1. Субъекты критической информационной инфраструктуры Российской Федерации имеют право:

1) в установленном порядке получать от уполномоченных федеральных органов исполнительной власти информацию, касающуюся обеспечения безопасности объектов критической информационной инфраструктуры Российской Федерации, принадлежащих им на праве собственности или ином законном основании;

2) самостоятельно разрабатывать мероприятия по обеспечению безопасности объекта критической информационной инфраструктуры Российской Федерации, не противоречащие требованиям настоящего Федерального закона и принятых в соответствии с ним нормативных правовых актов.

2. Субъекты критической информационной инфраструктуры Российской Федерации обязаны:

1) обеспечивать защиту, в том числе физическую, объектов критической информационной инфраструктуры Российской Федерации, принадлежащих им на праве собственности или ином законном основании;

2) направлять сведения о выполнении мероприятий, содержащихся в предписании по результатам проведенной оценки защищенности объектов критической информационной инфраструктуры Российской Федерации в уполномоченный федеральный орган исполнительной власти, определенный частью 7 статьи 9 настоящего Федерального закона;

3) незамедлительно информировать в порядке, установленном федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, о компьютерных инцидентах, произошедших на объектах критической информационной инфраструктуры Российской Федерации, принадлежащих им на праве собственности или ином законном основании;

4) выполнять предписания, представления должностных лиц уполномоченных федеральных органов исполнительной власти об устранении нарушений требований по обеспечению безопасности объекта критической информационной инфраструктуры Российской Федерации и об устранении причин и условий, способствующих реализации угроз безопасности Российской Федерации;

5) обеспечивать беспрепятственный доступ должностных лиц уполномоченных федеральных органов исполнительной власти к объекту критической информационной инфраструктуры Российской Федерации, при реализации ими полномочий, предусмотренных настоящим Федеральным законом;

6) оказывать содействие должностным лицам федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности, в выявлении, предупреждении и пресечении компьютерных инцидентов, а также в ликвидации их последствий, установлении причин и условий их совершения.

7) обеспечивать выполнение технических условий, порядка установки и эксплуатации, а также сохранность технических средств государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

8) обеспечивать выполнение технических условий, порядка установки и эксплуатации, а также сохранность технических средств, предназначенных для поиска признаков компьютерных атак в сообщениях электросвязи.

Статья 13. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

1. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации обеспечивает:

- организацию защиты информационных ресурсов Российской Федерации от компьютерных атак;
- выявление признаков проведения компьютерных атак, определение их источников, методов осуществления и направленности;
- организацию и осуществление взаимодействия на национальном и межгосударственном уровнях в области обнаружения компьютерных атак и установления их источников;
- научные исследования в области создания средств и методов обнаружения, предупреждения и ликвидации последствий компьютерных атак;
- сбор и анализ информации о компьютерных инцидентах в информационном пространстве Российской Федерации, а также о компьютерных инцидентах в информационном пространстве других стран, в которые вовлечены информационные ресурсы Российской Федерации;
- осуществление мероприятий по оперативному реагированию на компьютерные инциденты;
- организацию и осуществление взаимодействия с субъектами критической информационной инфраструктуры Российской Федерации, правоохранительными органами и другими заинтересованными органами и организациями по вопросам реагирования на компьютерные инциденты;
- сбор и анализ сведений о выявляемых уязвимостях программного обеспечения и оборудования, а также средствах и способах проведения компьютерных атак;
- организацию и осуществление международного обмена информацией о выявленных угрозах, обмене лучшими практиками выявления и устранения уязвимостей и реагирования на компьютерные инциденты;
- оценку реального уровня защищенности информационных систем и информационно-телекоммуникационных сетей;
- поиск и выявление компьютерных атак, а также ликвидация последствий компьютерных инцидентов.

4. В рамках государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации функционирует Национальный координационный центр по компьютерным инцидентам, обеспечение деятельности которого осуществляет федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности.

5. Представление информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации осуществляют:

субъекты критической информационной инфраструктуры Российской Федерации;

уполномоченные федеральные органы исполнительной власти, в том числе с использованием технических средств государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;

иные органы государственной власти;

аккредитованные организации, осуществляющие деятельность по оценке защищенности объектов критической информационной инфраструктуры Российской Федерации;

Перечень сведений, подлежащих представлению в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных инцидентов на информационные ресурсы Российской Федерации, и порядок их предоставления устанавливает федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности.

6. Сведения, содержащиеся в государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, относятся к информации ограниченного доступа. Если федеральным законом такие сведения отнесены к сведениям, составляющим государственную тайну, они подлежат защите в соответствии с законодательством Российской Федерации о государственной тайне.

Порядок доступа к информации, содержащейся в государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, определяется федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности.

7. Требования к техническим средствам, обеспечивающим взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, а также к техническим средствам, предназначенным для поиска признаков компьютерных атак в сообщениях электросвязи устанавливаются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации, по согласованию с федеральным органом исполнительной власти в области обеспечения безопасности.

8. Субъектами критической информационной инфраструктуры Российской Федерации в незамедлительном порядке принимаются меры по ликвидации последствий компьютерных инцидентов. Порядок реагирования на компьютерные инциденты и ликвидации их последствий на объектах критической информационной инфраструктуры Российской Федерации определяется федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности.

9. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации может использоваться для решения задач, не связанных с обеспечением безопасности объектов критической инфраструктуры Российской Федерации, в случаях, определенных в соответствии с частью первой статьи 6 настоящего Федерального закона.

Статья 14. Обеспечение безопасности объекта критической информационной инфраструктуры Российской Федерации

1. В целях обеспечения безопасности объектов критической информационной инфраструктуры Российской Федерации субъекты критической информационной инфраструктуры Российской Федерации создают на них системы безопасности и обеспечивают их функционирование.

2. Система безопасности объекта критической информационной инфраструктуры Российской Федерации должна обеспечивать:

1) предотвращение неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления,

распространения информации, а также совершения иных противоправных действий по отношению к информации, обеспечивающей управление и контроль за технологическими процессами критически важных объектов;

2) недопущение воздействия на технические средства обработки информации, в результате которого может быть нарушено или прекращено функционирование критической информационной инфраструктуры Российской Федерации;

3) реагирование на компьютерные инциденты;

4) возможность незамедлительного восстановления информации и функционирования объекта критической информационной инфраструктуры Российской Федерации;

5) создание и хранение резервных копий информации, обеспечивающей управление и контроль за технологическими процессами критически важных объектов;

6) непрерывное взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

3. Обеспечение физической защиты объекта критической информационной инфраструктуры Российской Федерации осуществляется в соответствии с законодательством Российской Федерации.

Глава 4. Контроль за соблюдением требований настоящего Федерального закона и ответственность за нарушение его требований

Статья 15. Государственный контроль (надзор) за соблюдением требований настоящего Федерального закона

1. Государственный контроль (надзор) в области безопасности критической информационной инфраструктуры Российской Федерации осуществляется в целях реализации принципов, установленных настоящим Федеральным законом.

2. Основанием для проведения плановой проверки является истечение трех лет со дня:

1) категорирования объекта критической информационной инфраструктуры Российской Федерации;

2) окончания проведения последней плановой проверки.

3. Основанием для проведения внеплановой проверки является:

1) истечение срока исполнения субъектом критической информационной инфраструктуры Российской Федерации выданного уполномоченным федеральным органом исполнительной власти предписания об устранении выявленного нарушения требований по обеспечению безопасности критической информационной инфраструктуры Российской Федерации;

2) поступление в уполномоченные органы исполнительной власти обращений и заявлений граждан, индивидуальных предпринимателей, юридических лиц, информации от органов государственной власти (в том числе должностных лиц уполномоченных органов исполнительной власти), органов местного самоуправления, из средств массовой информации и оперативных источников об угрозах возникновения компьютерных инцидентов на объектах критической информационной инфраструктуры Российской Федерации;

3) возникновение компьютерного инцидента на объекте критической информационной инфраструктуры Российской Федерации, повлекшего за собой нарушение или прекращение функционирования этого объекта;

4) наличие приказа (распоряжения) руководителя уполномоченного федерального органа исполнительной власти, изданного в соответствии с поручениями Президента Российской Федерации, Правительства Российской Федерации и на основании требования прокурора о проведении внеплановой проверки в рамках надзора за исполнением законов по поступившим в органы прокуратуры материалам и обращениям.

Статья 16. Ответственность за нарушение настоящего Федерального закона
За нарушение законодательства о безопасности критической информационной инфраструктуры Российской Федерации виновные лица несут дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

Глава 5. Заключительные и переходные положения

Статья 17. Вступление в силу настоящего Федерального закона
Настоящий Федеральный закон вступает в силу с 1 января 2015 года.
Президент
Российской Федерации
Москва, Кремль

6. Япония

サイバーセキュリティ基本法（暫定版）
The Basic Act on Cybersecurity (Tentative translation)
[неофициальный перевод на английский]
(http://www.japaneselawtranslation.go.jp/law/detail/?ft=1&re=02&dn=1&x=0&y=0&co=01&ia=03&ky=%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3&page=1)

平成二十六年十一月十二日法律第百四号
Act No. 104 of November 12, 2014

第一章　総則
Chapter I General Provisions

（目的）
(Purpose)

第一条　この法律は、インターネットその他の高度情報通信ネットワークの整備及び情報通信技術の活用の進展に伴って世界的規模で生じているサイバーセキュリティに対する脅威の深刻化その他の内外の諸情勢の変化に伴い、情報の自由な流通を確保しつつ、サイバーセキュリティの確保を図ることが喫緊の課題となっている状況に鑑み、我が国のサイバーセキュリティに関する施策に関し、基本理念を定め、国及び地方公共団体の責務等を明らかにし、並びにサイバーセキュリティ戦略の策定その他サイバーセキュリティに関する施策の基本となる事項を定めるとともに、サイバーセキュリティ戦略本部を設置すること等により、高度情報通信ネットワーク社会形成基本法（平成十二年法律第百四十四号）と相まって、サイバーセキュリティに関する施策を総合的かつ効果的に推進し、もって経済社会の活力の向上及び持続的発展並びに国民が安全で安心して暮らせる社会の実現を図るとともに、国際社会の平和及び安全の確保並びに我が国の安全保障に寄与することを目的とする。

Article 1　Facing domestic and foreign changes such as the intensification of threats against cybersecurity on a worldwide scale, and with the establishment of the Internet andother advanced information and telecommunications networks and the utilization of information and telecommunications technologies, and given the situation that it is an urgent issue to ensure the free flow of information and protect cybersecurity simultaneously, the purpose of this Act is to comprehensively and effectively promote cybersecurity policy by: stipulating basic principles of national cybersecurity policy; clarifying the responsibilities of the Government of Japan (hereinafter referred to as the"Government"), local governments, and other concerned public parties; stipulating essential matters for cybersecurity-related policies such as cybersecurity strategyformulation; and establishing the Cybersecurity Strategic Headquarters and so forth, together with the Basic Act on the Formation of an Advanced Information and Telecommunications Network Society (Act. No. 144 of 2000), and as a result, attempting to enhance economic and social vitality, sustainable development and realizing socialconditions where citizens can live with a sense of safety and security, and contributing to the protection of international peace and security as well as national security.

（定義）
(Definitions)
第二条　この法律において「サイバーセキュリティ」とは、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式（以下この条において「電磁的方式」という。）により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置（情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体（以下「電磁的記録媒体」という。）を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。）が講じられ、その状態が適切に維持管理されていることをいう。
Article 2 For the purposes of this Act, the term "Cybersecurity" means that necessary measures are taken: to safely manage information, such as prevent against the leakage, disappearance, or damage of information which is stored, sent, in transmission, or received by electronic, magnetic, or other means unrecognizable by natural perceptive function (hereinafter in this section referred to as "electro-magnetic means"); and to guarantee the safety and reliability of information systems and information andtelecommunications networks (including necessary preventive measures against malicious activities toward electronic computers through information network or storage media for information created by electro-magnetic means [hereinafter referred to as "electro-magnetic storage media"]), and that those states are appropriately maintained.
（基本理念）
(Basic Principles)
第三条　サイバーセキュリティに関する施策の推進は、インターネットその他の高度情報通信ネットワークの整備及び情報通信技術の活用による情報の自由な流通の確保が、これを通じた表現の自由の享有、イノベーションの創出、経済社会の活力の向上等にとって重要であることに鑑み、サイバーセキュリティに対する脅威に対して、国、地方公共団体、重要社会基盤事業者（国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるものに関する事業を行う者をいう。以下同じ。）等の多様な主体の連携により、積極的に対応することを旨として、行われなければならない。
Article 3 (1) Given that ensuring the free flow of information through the maintenance of advanced information and telecommunications networks such as the Internet andthe utilization of information and telecommunications technologies is critical to enjoying benefits from the freedom of expression, enabling the creation of innovation, improving economic and social vitality, and so on, the promotion of cybersecurity policy shall be required to be carried out with intent to produce active responses to threats against cybersecurity through coordination among multiple stakeholders, including the Government, local governments, and critical information infrastructure (CII) operators (here and hereinafter referring to operators of businesses that provide infrastructure which is the basis of citizen's living conditions and economic activities and the functional failure or deterioration of which would risk enormous impacts to them; hereinafter referred to as "CII operators").
２　サイバーセキュリティに関する施策の推進は、国民一人一人のサイバーセキュリティに関する認識を深め、自発的に対応することを促すとともに、サイバーセキ

ュリティに対する脅威による被害を防ぎ、かつ、被害から迅速に復旧できる強靱（じん）な体制を構築するための取組を積極的に推進することを旨として、行われなければならない。
(2) The promotion of cybersecurity policy shall be required to be carried out with intent to raise awareness of each citizen about cybersecurity and invite each citizen's voluntary actions to prevent any damage caused by threats against cybersecurity, and to positively promote actions to establish resilient systems which can quickly recover from damage or failure.
３　サイバーセキュリティに関する施策の推進は、インターネットその他の高度情報通信ネットワークの整備及び情報通信技術の活用による活力ある経済社会を構築するための取組を積極的に推進することを旨として、行われなければならない。
(3) The promotion of cybersecurity policy shall be required to be carried out with intent to positively implement the maintenance of the Internet and other advanced information and telecommunications networks and actions toward the establishment of a vital economy and society through the utilization of information andtelecommunications technologies.
４　サイバーセキュリティに関する施策の推進は、サイバーセキュリティに対する脅威への対応が国際社会にとって共通の課題であり、かつ、我が国の経済社会が国際的な密接な相互依存関係の中で営まれていることに鑑み、サイバーセキュリティに関する国際的な秩序の形成及び発展のために先導的な役割を担うことを旨として、国際的協調の下に行われなければならない。
(4) Given that combatting threats against cybersecurity is a common concern of the international community, and with recognition that Japan's economic and social activities are characterized by close international interdependence, the promotion of cybersecurity policy shall be required to be carried out with intent to play a leading role in an internationally-coordinated effort for the creation and development of an international normative framework for cybersecurity.
５　サイバーセキュリティに関する施策の推進は、高度情報通信ネットワーク社会形成基本法の基本理念に配慮して行われなければならない。
(5) The promotion of cybersecurity policy shall be required to be carried out in consideration of the basic principles of the Basic Act on the Formation of an Advanced Information and Telecommunications Network Society.
６　サイバーセキュリティに関する施策の推進に当たっては、国民の権利を不当に侵害しないように留意しなければならない。
(6) The promotion of the cybersecurity policy shall be required to be carried out with intent to be careful not to wrongfully impinge upon citizens' rights.
（国の責務）
(Responsibility of the Government)
第四条　国は、前条の基本理念（以下「基本理念」という。）にのっとり、サイバーセキュリティに関する総合的な施策を策定し、及び実施する責務を有する。
Article 4 In accordance with the basic principles prescribed under the preceding article, (hereinafter referred to as the "basic principles"), the Government shall bear theresponsibility to formulate and implement comprehensive cybersecurity policies.
（地方公共団体の責務）
(Responsibility of Local Governments)

第五条　地方公共団体は、基本理念にのっとり、国との適切な役割分担を踏まえて、サイバーセキュリティに関する自主的な施策を策定し、及び実施する責務を有する。
Article 5 In accordance with the basic principles, local governments shall bear the responsibility to formulate and implement proactive cybersecurity policies in consideration of the appropriate division of roles with the Government.
（重要社会基盤事業者の責務）
(Responsibility of CII Operators)
第六条　重要社会基盤事業者は、基本理念にのっとり、そのサービスを安定的かつ適切に提供するため、サイバーセキュリティの重要性に関する関心と理解を深め、自主的かつ積極的にサイバーセキュリティの確保に努めるとともに、国又は地方公共団体が実施するサイバーセキュリティに関する施策に協力するよう努めるものとする。
Article 6 In accordance with the basic principles and for the purpose of stable and appropriate provision of their services, CII operators shall make an effort to: deepen their awareness and understanding of the critical value of cybersecurity; assure cybersecurity voluntarily and proactively; and cooperate with the measures on cybersecurity taken by the Government or local governments.
（サイバー関連事業者その他の事業者の責務）
(Responsibility of Cyberspace-related Business Entities and Other Business Entities)
第七条　サイバー関連事業者（インターネットその他の高度情報通信ネットワークの整備、情報通信技術の活用又はサイバーセキュリティに関する事業を行う者をいう。以下同じ。）その他の事業者は、基本理念にのっとり、その事業活動に関し、自主的かつ積極的にサイバーセキュリティの確保に努めるとともに、国又は地方公共団体が実施するサイバーセキュリティに関する施策に協力するよう努めるものとする。
Article 7 In accordance with the basic principles, cyberspace-related business entities (here and hereinafter, referring to those engaged in business regarding the maintenanceof the Internet and other advanced information and telecommunications networks, the utilization of information and telecommunications technologies, or involved in businessrelated to cybersecurity) and other business entities shall make an effort to assure cybersecurity voluntarily and proactively in their businesses and to cooperate with themeasures on cybersecurity taken by the Government or local governments.
（教育研究機関の責務）
(Responsibility of Educational and Research Organizations)
第八条　大学その他の教育研究機関は、基本理念にのっとり、自主的かつ積極的にサイバーセキュリティの確保、サイバーセキュリティに係る人材の育成並びにサイバーセキュリティに関する研究及びその成果の普及に努めるとともに、国又は地方公共団体が実施するサイバーセキュリティに関する施策に協力するよう努めるものとする。
Article 8 In accordance with the basic principles, universities and other educational and research organizations shall make an effort to assure cybersecurity voluntarily andproactively, develop human resources specialized for cybersecurity, disseminate research and the results of research on cybersecurity, and cooperate with measures taken by the Government or local governments.

（国民の努力）
(Citizens' Efforts)
第九条　国民は、基本理念にのっとり、サイバーセキュリティの重要性に関する関心と理解を深め、サイバーセキュリティの確保に必要な注意を払うよう努めるものとする。
Article 9　In accordance with the basic principles, citizens shall make an effort to deepen their awareness and understanding of the critical value of cybersecurity and pay necessary attention to assuring cybersecurity.
（法制上の措置等）
(Legislative and Other Measures)
第十条　政府は、サイバーセキュリティに関する施策を実施するため必要な法制上、財政上又は税制上の措置その他の措置を講じなければならない。
Article 10 The Government shall be required to take necessary measures for the implementation of cybersecurity policies including legislative, financial, or taxation measures.
（行政組織の整備等）
(Development of Administrative Organizations, and so forth)
第十一条　国は、サイバーセキュリティに関する施策を講ずるにつき、行政組織の整備及び行政運営の改善に努めるものとする。
Article 11　In providing cybersecurity policies, the Government shall make an effort to develop administrative organizations and to improve administrative management.
第二章　サイバーセキュリティ戦略
Chapter II The Cybersecurity Strategy
第十二条　政府は、サイバーセキュリティに関する施策の総合的かつ効果的な推進を図るため、サイバーセキュリティに関する基本的な計画（以下「サイバーセキュリティ戦略」という。）を定めなければならない。
Article 12 (1) The Government shall be required to establish a basic plan for cybersecurity (hereinafter referred to as the "Cybersecurity Strategy") with the aim of thecomprehensive and effective promotion of cybersecurity policy.
２　サイバーセキュリティ戦略は、次に掲げる事項について定めるものとする。
(2) The Cybersecurity Strategy shall address the following:
一　サイバーセキュリティに関する施策についての基本的な方針
(i) Basic objectives of cybersecurity policies;
二　国の行政機関等におけるサイバーセキュリティの確保に関する事項
(ii) Matters regarding cybersecurity assurance within national administrative organs and other related organs;
三　重要社会基盤事業者及びその組織する団体並びに地方公共団体（以下「重要社会基盤事業者等」という。）におけるサイバーセキュリティの確保の促進に関する事項
(iii) Matters regarding the promotion of cybersecurity assurance at CII operators, their professional associations, and local governments (hereinafter referred to as "CII operators and other related entities");
四　前三号に掲げるもののほか、サイバーセキュリティに関する施策を総合的かつ効果的に推進するために必要な事項
(iv) In addition to the matters listed in the preceding three items, other matters required for the comprehensive and effective promotion of cybersecurity policies.

３　内閣総理大臣は、サイバーセキュリティ戦略の案につき閣議の決定を求めなければならない。
(3) The Prime Minister shall be required to request a cabinet decision on the proposed Cybersecurity Strategy.
４　政府は、サイバーセキュリティ戦略を策定したときは、遅滞なく、これを国会に報告するとともに、インターネットの利用その他適切な方法により公表しなければならない。
(4) When establishing the Cybersecurity Strategy, the Government shall be required to report it to the Diet without delay and to announce it publicly by using the Internet andother appropriate means.
５　前二項の規定は、サイバーセキュリティ戦略の変更について準用する。
(5) The provisions prescribed under the preceding two paragraphs shall apply in the case of amendments to the Cybersecurity Strategy.
６　政府は、サイバーセキュリティ戦略について、その実施に要する経費に関し必要な資金の確保を図るため、毎年度、国の財政の許す範囲内で、これを予算に計上する等その円滑な実施に必要な措置を講ずるよう努めなければならない。
(6) With the aim of assuring necessary funds regarding the expenses to enable the implementation of the Cybersecurity Strategy, the Government shall be required to make an effort to provide necessary measures for the smooth implementation of the Cybersecurity Strategy, such as appropriating the necessary funds in its budget every fiscal year, to the extent permitted within national fiscal limitations.

第三章　基本的施策
Chapter III Basic Policy

（国の行政機関等におけるサイバーセキュリティの確保）
(Assurance of Cybersecurity at National Administrative Organs and Related Organs)

第十三条　国は、国の行政機関、独立行政法人（独立行政法人通則法（平成十一年法律第百三号）第二条第一項に規定する独立行政法人をいう。以下同じ。）及び特殊法人（法律により直接に設立された法人又は特別の法律により特別の設立行為をもって設立された法人であって、総務省設置法（平成十一年法律第九十一号）第四条第十五号の規定の適用を受けるものをいう。以下同じ。）等におけるサイバーセキュリティに関し、国の行政機関及び独立行政法人におけるサイバーセキュリティに関する統一的な基準の策定、国の行政機関における情報システムの共同化、情報通信ネットワーク又は電磁的記録媒体を通じた国の行政機関の情報システムに対する不正な活動の監視及び分析、国の行政機関におけるサイバーセキュリティに関する演習及び訓練並びに国内外の関係機関との連携及び連絡調整によるサイバーセキュリティに対する脅威への対応、国の行政機関、独立行政法人及び特殊法人等の間におけるサイバーセキュリティに関する情報の共有その他の必要な施策を講ずるものとする。
Article 13 With regard to cybersecurity at national administrative organs, incorporated administrative agencies (here and hereinafter referring to incorporated administrative agencies prescribed under Article 2, paragraph (1) of the Act on General Rules for Incorporated Administrative Agencies [Act No. 103 of 1999]), special corporations (hereand hereinafter referring to juridical persons directly incorporated by acts or juridical persons incorporated by a special act pursuant to a special incorporation procedure andsubject to the provision of Article 4 (xv) of the Act for Establishment of the Ministry of Internal Affairs and Communications [Act No. 91

of 1999]), and so forth, theGovernment shall provide necessary measures including: the formulation of common standards of cybersecurity measures for national administrative organs and incorporated administrative agencies; the collaborative use of interoperable information systems among national administrative organs; monitoring and analysis of malicious activities against information systems of national administrative organs through information and communications networks or electro-magnetic storage media; cybersecurity exercisesand training at national administrative organs; responses to cybersecurity threats in cooperation, communication and coordination with relevant domestic and foreign parties;the sharing of information about cybersecurity among national administrative organs, incorporated administrative agencies, special corporations, and so forth.

（重要社会基盤事業者等におけるサイバーセキュリティの確保の促進）

(Assurance of Cybersecurity at CII Operators and Other Related Entities)

第十四条　国は、重要社会基盤事業者等におけるサイバーセキュリティに関し、基準の策定、演習及び訓練、情報の共有その他の自主的な取組の促進その他の必要な施策を講ずるものとする。

Article 14 With regard to cybersecurity at CII operators and other related entities, the Government shall provide necessary measures, including the formulation of standards, exercises and training, the promotion of information sharing and other voluntary activities.

（民間事業者及び教育研究機関等の自発的な取組の促進）

(Facilitation of Voluntary Activities of Private Enterprises, Educational, Research, and Other Organizations)

第十五条　国は、中小企業者その他の民間事業者及び大学その他の教育研究機関が有する知的財産に関する情報が我が国の国際競争力の強化にとって重要であることに鑑み、これらの者が自発的に行うサイバーセキュリティに対する取組が促進されるよう、サイバーセキュリティの重要性に関する関心と理解の増進、サイバーセキュリティに関する相談に応じ、必要な情報の提供及び助言を行うことその他の必要な施策を講ずるものとする。

Article 15 (1) Given that information on intellectual property owned by private enterprises such as small and medium-sized enterprises and educational and research organizations such as universities is critical for the enhancement of Japan's international competitiveness, and in order to promote their voluntary activities for cybersecurity,the Government shall provide necessary measures, including increasing awareness and understanding about the critical value of cybersecurity, offering consultation on cybersecurity, and providing necessary information and advice.

２　国は、国民一人一人が自発的にサイバーセキュリティの確保に努めることが重要であることに鑑み、日常生活における電子計算機又はインターネットその他の高度情報通信ネットワークの利用に際して適切な製品又はサービスを選択することその他の取組について、サイバーセキュリティに関する相談に応じ、必要な情報の提供及び助言を行うことその他の必要な施策を講ずるものとする。

(2) Given that it is important for each citizen to make an effort to voluntarily assure cybersecurity, the Government shall provide necessary measures,
including offeringconsultation on cybersecurity and providing necessary information and advice on actions such as, appropriate choices about products and services in the daily use of electronic computers or the Internet and other advanced information and telecommunications networks.

（多様な主体の連携等）
(Coordination with Multiple Stakeholders, and so forth)
第十六条　国は、関係府省相互間の連携の強化を図るとともに、国、地方公共団体、重要社会基盤事業者、サイバー関連事業者等の多様な主体が相互に連携してサイバーセキュリティに関する施策に取り組むことができるよう必要な施策を講ずるものとする。
Article 16 The Government shall aim at the enhancement of coordination among relevant ministries and shall provide necessary measures to enable multiple stakeholders,such as the Government, local governments, CII operators, and cyberspace-related business entities, to work on cybersecurity policies in mutual coordination.
（犯罪の取締り及び被害の拡大の防止）
(Crackdown on Cybercrime and Prevention of Damage)
第十七条　国は、サイバーセキュリティに関する犯罪の取締り及びその被害の拡大の防止のために必要な施策を講ずるものとする。
Article 17 The Government shall provide necessary measures to crackdown on cybercrime and prevent the spread of damage.
（我が国の安全に重大な影響を及ぼすおそれのある事象への対応）
(Action for Matters Which May Critically Affect the Country's Safety)
第十八条　国は、サイバーセキュリティに関する事象のうち我が国の安全に重大な影響を及ぼすおそれがあるものへの対応について、関係機関における体制の充実強化並びに関係機関相互の連携強化及び役割分担の明確化を図るために必要な施策を講ずるものとする。
Article 18 The Government shall provide necessary measures with the intention to: improve and strengthen systems to respond cybersecurity concerns at relevant bodies; strengthen the mutual coordination among relevant bodies; and clarify the division of roles among relevant bodies, as actions to address threats which may critically affect thecountry's safety with respect to cybersecurity-related incidents.
（産業の振興及び国際競争力の強化）
(Enhancement of Industrial Development and International Competitiveness)
第十九条　国は、サイバーセキュリティの確保を自立的に行う能力を我が国が有することの重要性に鑑み、サイバーセキュリティに関連する産業が雇用機会を創出することができる成長産業となるよう、新たな事業の創出並びに産業の健全な発展及び国際競争力の強化を図るため、サイバーセキュリティに関し、先端的な研究開発の推進、技術の高度化、人材の育成及び確保、競争条件の整備等による経営基盤の強化及び新たな事業の開拓、技術の安全性及び信頼性に係る規格等の国際標準化及びその相互承認の枠組みへの参画その他の必要な施策を講ずるものとする。
Article 19 Given that it is critical for Japan to have self-reliant capabilities to assure cybersecurity, and in order to create new business opportunities, develop businesses thatare sound, and improve international competitiveness, and so as to make the cybersecurity sector a "growth industry" which is able to create employment opportunities, theGovernment shall provide necessary measures related to cybersecurity, including the promotion of advanced research and development, technological advancements, thedevelopment and recruitment of human resources, the strengthening of the market environment and the development of new businesses through the improvement of competitive conditions, and the internationalization of technological safety and reliability standards and the participation in such frameworks on the basis of mutualrecognition.

（研究開発の推進等）
(Promotion of Research and Development, and so forth)
第二十条　国は、我が国においてサイバーセキュリティに関する技術力を自立的に保持することの重要性に鑑み、サイバーセキュリティに関する研究開発及び技術等の実証の推進並びにその成果の普及を図るため、サイバーセキュリティに関し、研究体制の整備、技術の安全性及び信頼性に関する基礎研究及び基盤的技術の研究開発の推進、研究者及び技術者の育成、国の試験研究機関、大学、民間等の連携の強化、研究開発のための国際的な連携その他の必要な施策を講ずるものとする。
Article 20 Given that it is critical for Japan to maintain self-reliant technological cybersecurity capabilities, in order to promote research and development for cybersecurity as well as the technological and other relevant demonstrations of cybersecurity, and to expand the distribution of relevant cybersecurity outcomes, the Government shall providenecessary measures related to cybersecurity for: the improvement of the environment of cybersecurity research; the promotion of basic research on technological safetyand reliability as well as the promotion of research and development for core technologies; the development of skilled researchers and engineers; the strengthening of coordination among national research institutes, universities, the private sector, and other relevant parties; and international coordination for research and development.
（人材の確保等）
(Development of Human Resources, and so forth)
第二十一条　国は、大学、高等専門学校、専修学校、民間事業者等と緊密な連携協力を図りながら、サイバーセキュリティに係る事務に従事する者の職務及び職場環境がその重要性にふさわしい魅力あるものとなるよう、当該者の適切な処遇の確保に必要な施策を講ずるものとする。
Article 21 (1) In close coordination and cooperation with universities, colleges of technology, specialized training colleges, private enterprises, and other relevant entities, theGovernment shall provide necessary measures to assure appropriate assignments and employment conditions or treatment of the workforce in the field of cybersecurity, thereby enabling their functions and work environments to become attractive enough to meet their professional values.
２　国は、大学、高等専門学校、専修学校、民間事業者等と緊密な連携協力を図りながら、サイバーセキュリティに係る人材の確保、養成及び資質の向上のため、資格制度の活用、若年技術者の養成その他の必要な施策を講ずるものとする。
(2) In close coordination and cooperation with universities, colleges of technology, specialized training colleges, private enterprises, and other relevant entities, for the purposes of the recruitment, development, and quality improvement of cybersecurity-related human resources, the Government shall provide necessary measures, including theutilization of a qualification scheme and training of young technical experts.
（教育及び学習の振興、普及啓発等）
(Promotion of Education and Learning, Public Awareness Raising, and so forth)
第二十二条　国は、国民が広くサイバーセキュリティに関する関心と理解を深めるよう、サイバーセキュリティに関する教育及び学習の振興、啓発及び知識の普及その他の必要な施策を講ずるものとする。
Article 22 (1) For the purpose of extensive public awareness raising and understanding about cybersecurity among the citizens, the Government shall provide necessarymeasures

including the promotion of education and learning, public awareness activities, and the dissemination of knowledge in the field of cybersecurity.
２　国は、前項の施策の推進に資するよう、サイバーセキュリティに関する啓発及び知識の普及を図るための行事の実施、重点的かつ効果的にサイバーセキュリティに対する取組を推進するための期間の指定その他の必要な施策を講ずるものとする。
(2) In order to promote the measures prescribed under the preceding paragraph, the Government shall provide necessary measures, including the implementation of events forpublic awareness and the dissemination of information on cybersecurity and the designation of a specific, focused campaign period to effectively promote cybersecurity activities.
（国際協力の推進等）
(Promotion of International Cooperation, and so forth)
第二十三条　国は、サイバーセキュリティに関する分野において、我が国の国際社会における役割を積極的に果たすとともに、国際社会における我が国の利益を増進するため、サイバーセキュリティに関し、国際的な規範の策定への主体的な参画、国際間における信頼関係の構築及び情報の共有の推進、開発途上地域のサイバーセキュリティに関する対応能力の構築の積極的な支援その他の国際的な技術協力、犯罪の取締りその他の国際協力を推進するとともに、我が国のサイバーセキュリティに対する諸外国の理解を深めるために必要な施策を講ずるものとする。
Article 23　In the field of cybersecurity, to actively carry out Japan's role in the international community and to promote Japan's interests in the community, the Governmentshall promote: active participation in international norm setting; confidence building and the promotion of information sharing with foreign countries; international technical cooperation such as active support for cybersecurity capacity building in developing countries; international cooperation such as crackdowns on cybercrime; and shallprovide necessary measures to deepen other countries' understanding of Japan's cybersecurity.
第四章　サイバーセキュリティ戦略本部
Chapter IV Cybersecurity Strategic Headquarters
（設置）
(Establishment)
第二十四条　サイバーセキュリティに関する施策を総合的かつ効果的に推進するため、内閣に、サイバーセキュリティ戦略本部（以下「本部」という。）を置く。
Article 24　For the purpose of effectively and comprehensively promoting cybersecurity policies, the Cybersecurity Strategic Headquarters (hereinafter referred to as the "Headquarters") shall be established under the Cabinet.
（所掌事務等）
(Functions under Jurisdiction of the Headquarters)
第二十五条　本部は、次に掲げる事務をつかさどる。
Article 25　(1)　The Headquarters shall perform functions as follows:
一　サイバーセキュリティ戦略の案の作成及び実施の推進に関すること。
(i)　Preparing the Cybersecurity Strategy and promoting its implementation.
二　国の行政機関及び独立行政法人におけるサイバーセキュリティに関する対策の基準の作成及び当該基準に基づく施策の評価（監査を含む。）その他の当該基準に基づく施策の実施の推進に関すること。
(ii) Establishing the standards of cybersecurity measures for national administrative organs and incorporated administrative

agencies, and promoting the implementation of theevaluation (including audit) of measures based on the said standards and other measures taken pursuant to the said standards.

三　国の行政機関で発生したサイバーセキュリティに関する重大な事象に対する施策の評価（原因究明のための調査を含む。）に関すること。

(iii) Evaluating the countermeasures against critical cybersecurity-related incidents involving national administrative organs (including fact-finding activities to determine thecause or causes of the incident).

四　前三号に掲げるもののほか、サイバーセキュリティに関する施策で重要なものの企画に関する調査審議、府省横断的な計画、関係行政機関の経費の見積りの方針及び施策の実施に関する指針の作成並びに施策の評価その他の当該施策の実施の推進並びに総合調整に関すること。

(iv) In addition to the functions listed in the preceding three items, with respect to major cybersecurity policies: engaging in research and deliberation on program proposals; establishing cross-governmental plans, budget plans and guidelines of relevant administrative organs, and the basic principles of program implementation as well as promotingthe implementation of policy evaluation and other relevant policies; and carrying out overall coordination.

２　本部は、サイバーセキュリティ戦略の案を作成しようとするときは、あらかじめ、高度情報通信ネットワーク社会推進戦略本部及び国家安全保障会議の意見を聴かなければならない。

(2) In preparing the draft Cybersecurity Strategy, the Headquarters shall be required to consult with the Strategic Headquarters for the Promotion of an Advanced Information Telecommunications Network Society, and the National Security Council in advance.

３　本部は、サイバーセキュリティに関する重要事項について、高度情報通信ネットワーク社会推進戦略本部との緊密な連携を図るものとする。

(3) The Headquarters shall work in close coordination with the Strategic Headquarters for the Promotion of an Advanced Information Telecommunications Network Society with regard to critical issues concerning cybersecurity.

４　本部は、我が国の安全保障に係るサイバーセキュリティに関する重要事項について、国家安全保障会議との緊密な連携を図るものとする。

(4) The Headquarters shall work in close coordination with the National Security Council with regard to critical issues concerning cybersecurity in the context of nationalsecurity.

（組織）

(Organization)

第二十六条　本部は、サイバーセキュリティ戦略本部長、サイバーセキュリティ戦略副本部長及びサイバーセキュリティ戦略本部員をもって組織する。

Article 26 The Headquarters shall consist of the Chief, the Deputy Chief, and the members of the Headquarters.

（サイバーセキュリティ戦略本部長）

(The Chief of the Cybersecurity Strategic Headquarters)

第二十七条　本部の長は、サイバーセキュリティ戦略本部長（以下「本部長」という。）とし、内閣官房長官をもって充てる。

Article 27 (1) The Chief Cabinet Secretary shall serve as the Chief of the Headquarters (hereinafter referred to as the "Chief")

２　本部長は、本部の事務を総括し、所部の職員を指揮監督する。

(2) The Chief shall engage in the overall management of the Headquarters' functions and the oversight of the personnel at the Headquarters.

３　本部長は、第二十五条第一項第二号から第四号までに規定する評価又は第三十条若しくは第三十一条の規定により提供された資料、情報等に基づき、必要があると認めるときは、関係行政機関の長に対し、勧告することができる。
(3) The Chief may, where necessary, make recommendations to the heads of relevant administrative organs, based on the evaluations prescribed under Article 25, paragraph(1), item (ii) to (iv), or the documents, information or other materials provided pursuant to the provisions under Articles 30 or 31.
４　本部長は、前項の規定により関係行政機関の長に対し勧告したときは、当該関係行政機関の長に対し、その勧告に基づいてとった措置について報告を求めることができる。
(4) After making the recommendations as prescribed under the preceding paragraph, the Chief may request a report from the heads of the relevant administrative organs regarding the measures taken based on the recommendations.
５　本部長は、第三項の規定により勧告した事項に関し特に必要があると認めるときは、内閣総理大臣に対し、当該事項について内閣法（昭和二十二年法律第五号）第六条の規定による措置がとられるよう意見を具申することができる。
(5) The Chief may, where particularly necessary in relation to the recommendations made in accordance with paragraph (3) of this article, present opinions for the Prime Minister to take an action for the said matter, as prescribed under Article 6 of the Cabinet Law (Act No. 5 of 1947).
（サイバーセキュリティ戦略副本部長）
(The Deputy Chief of the Cybersecurity Strategic Headquarters)
第二十八条　本部に、サイバーセキュリティ戦略副本部長（以下「副本部長」という。）を置き、国務大臣をもって充てる。
Article 28 (1) A Minster of State shall be designated as the Deputy Chief of the Cybersecurity Strategic Headquarters (hereinafter referred to as the "Deputy Chief")
２　副本部長は、本部長の職務を助ける。
(2) The Deputy Chief shall assist the Chief's missions.
（サイバーセキュリティ戦略本部員）
(Members of the Cybersecurity Strategic Headquarters)
第二十九条　本部に、サイバーセキュリティ戦略本部員（次項において「本部員」という。）を置く。
Article 29 (1) The Headquarters shall establish the members of the Cybersecurity Strategic Headquarters (referred to in the succeeding paragraph as the "members").
２　本部員は、次に掲げる者（第一号から第五号までに掲げる者にあっては、副本部長に充てられたものを除く。）をもって充てる。
(2) Those listed below shall be designated as the members (except in a case where someone listed in item (i) to (v) is designated as the Deputy Chief).
一　国家公安委員会委員長
(i) The Chairperson of the National Public Safety Commission;
二　総務大臣
(ii) The Minister for Internal Affairs and Communications;
三　外務大臣
(iii) The Minister for Foreign Affairs;
四　経済産業大臣
(iv) The Minister of Economy, Trade and Industry;

五　防衛大臣
(v)　The Minister of Defense;
六　前各号に掲げる者のほか、本部長及び副本部長以外の国務大臣のうちから、本部の所掌事務を遂行するために特に必要があると認める者として内閣総理大臣が指定する者
(vi)　In addition to those listed above, any Minister of State, except the Chief and the Deputy Chief, who is designated by the Prime Minister as indispensable for the functions of the Headquarters; and
七　サイバーセキュリティに関し優れた識見を有する者のうちから、内閣総理大臣が任命する者
(vii)　Among experts with exceptional knowledge and experiences on cybersecurity, those designated by the Prime Minister.
（資料提供等）
(Submission of Materials, and so forth)
第三十条　関係行政機関の長は、本部の定めるところにより、本部に対し、サイバーセキュリティに関する資料又は情報であって、本部の所掌事務の遂行に資するものを、適時に提供しなければならない。
Article 30 (1) As set by the Headquarters, the heads of the relevant administrative organs shall have a duty to furnish the Headquarters timely with materials and/orinformation regarding cybersecurity that are beneficial in fulfilling its functions.
２　前項に定めるもののほか、関係行政機関の長は、本部長の求めに応じて、本部に対し、本部の所掌事務の遂行に必要なサイバーセキュリティに関する資料又は情報の提供及び説明その他必要な協力を行わなければならない。
(2) In addition to the provision under the preceding paragraph, when requested by the Chief, the heads of the relevant administrative organs shall have a duty to cooperate withthe Headquarters for the fulfillment of its functions, by providing materials and/or information regarding cybersecurity, explanation and other necessary cooperation.
（資料の提出その他の協力）
(Submission of Materials and Other Cooperation)
第三十一条　本部は、その所掌事務を遂行するため必要があると認めるときは、地方公共団体及び独立行政法人の長、国立大学法人（国立大学法人法（平成十五年法律第百十二号）第二条第一項に規定する国立大学法人をいう。）の学長、大学共同利用機関法人（同条第三項に規定する大学共同利用機関法人をいう。）の機構長、日本司法支援センター（総合法律支援法（平成十六年法律第七十四号）第十三条に規定する日本司法支援センターをいう。）の理事長、特殊法人及び認可法人（特別の法律により設立され、かつ、その設立等に関し行政官庁の認可を要する法人をいう。）であって本部が指定するものの代表者並びにサイバーセキュリティに関する事象が発生した場合における国内外の関係者との連絡調整を行う関係機関の代表者に対して、資料の提出、意見の開陳、説明その他必要な協力を求めることができる。
Article 31 (1) The Headquarters may, where necessary for the fulfillment of its functions, request the submission of materials, the presentation of opinion, explanation andany other necessary cooperation from: the heads of local governments and incorporated administrative agencies; the deans of national university corporations (referring tonational university corporations prescribed under Article 2, paragraph (1) of the National University Corporation Act [Act

No.112 of 2003]); the heads of inter-universityresearch institute corporations (referring to inter-university research institute corporations prescribed under Article 2, paragraph (3) of the said Act); the President of theJapan Legal Support Center (referring to the Japan Legal Support Center prescribed under Article 13 of the Comprehensive Legal Support Act [Act No. 74 of 2004]); therepresentatives of special corporations and authorized corporations (referring to juridical persons incorporated by a special act and where the approval of a governmental entity is required for their incorporation and associated matters) designated by the Headquarters; and the representative of the relevant entity facilitating cybersecurity-relatedcommunication and coordination with domestic and foreign parties concerned.

２　本部は、その所掌事務を遂行するため特に必要があると認めるときは、前項に規定する者以外の者に対しても、必要な協力を依頼することができる。

(2) In addition, the Headquarters may, where particularly necessary for the fulfillment of its functions, request necessary cooperation from a party other than the parties prescribed in the preceding paragraph.

（地方公共団体への協力）

(Cooperation for Local Governments)

第三十二条　地方公共団体は、第五条に規定する施策の策定又は実施のために必要があると認めるときは、本部に対し、情報の提供その他の協力を求めることができる。

Article 32 (1) Local governments may, where necessary for the establishment and implementation of the policies prescribed under Article 5, request the provision of information and other cooperation from the Headquarters.

２　本部は、前項の規定による協力を求められたときは、その求めに応じるよう努めるものとする。

(2) When the cooperation is requested pursuant to the preceding paragraph, the Headquarters shall make an effort to meet the request.

（事務）

(Functions)

第三十三条　本部に関する事務は、内閣官房において処理し、命を受けて内閣官房副長官補が掌理する。

Article 33 The functions of the Headquarters shall be performed by the Cabinet Secretariat and managed by a designated Assistant Chief Cabinet Secretary.

（主任の大臣）

(Chief Minister)

第三十四条　本部に係る事項については、内閣法にいう主任の大臣は、内閣総理大臣とする。

Article 34 For matters pertaining to the Headquarters, the Prime Minister shall be the chief minister as prescribed in the Cabinet Act.

（政令への委任）

(Delegation to Cabinet Orders)

第三十五条　この法律に定めるもののほか、本部に関し必要な事項は、政令で定める。

Article 35 In addition to the provisions of this Act, necessary matters pertaining to the Headquarters shall be prescribed by a Cabinet Order.

附　則

Supplementary Provisions

（施行期日）

(Effective Date)
第一条　この法律は、公布の日から施行する。ただし、第二章及び第四章の規定並びに附則第四条の規定は、公布の日から起算して一年を超えない範囲内において政令で定める日から施行する。
Article 1 This Act shall come into effect as from the date of promulgation. However, the provisions of Chapters II and IV as well as Article 4 of the Supplementary Provisions shall come into effect from a day specified by a Cabinet Order within a period not exceeding one year from the date of promulgation.
（本部に関する事務の処理を適切に内閣官房に行わせるために必要な法制の整備等）
(Development of the Legal System Necessary to Enable the Cabinet Secretariat to Appropriately Perform the Headquarters-related Functions, and so forth)
第二条　政府は、本部に関する事務の処理を適切に内閣官房に行わせるために必要な法制の整備（内閣総理大臣の決定により内閣官房に置かれる情報セキュリティセンターの法制化を含む。）その他の措置を講ずるものとする。
Article 2 (1) The Government shall take necessary measures, such as the development of a legal system (including the legislation of the National Information Security Center, which is part of the Cabinet Secretariat, as determined by the Prime Minister) necessary to enable the Cabinet Secretariat to appropriately fulfill Headquarters-related functions.
２　政府は、前項の措置を講ずるに当たっては、専門的知識を有する者を内閣官房において任期を定めて職員又は研究員として任用すること、情報通信ネットワーク又は電磁的記録媒体を通じた国の行政機関の情報システムに対する不正な活動の監視及び分析並びにサイバーセキュリティに関する事象に関する国内外の関係機関との連絡調整に必要な機材及び人的体制の整備等のために必要な法制上及び財政上の措置等について検討を加え、その結果に基づいて必要な措置を講ずるものとする。
(2) In taking the measures prescribed under the preceding paragraph, the Government shall examine legislative and financial measures necessary for: the fixed-termappointments of specialists as staff members or researchers in the Cabinet Secretariat; the monitoring and analysis of malicious activities against the information systems of national governmental organs through information and telecommunications networks or electro-magnetic storage media; and the development of equipment andpersonnel systems required for communication and coordination with relevant domestic and foreign organizations on cybersecurity issues, and so forth, and shall take necessary measures based on the result of these examinations.
（検討）
(Examination)
第三条　政府は、武力攻撃事態等における我が国の平和と独立並びに国及び国民の安全の確保に関する法律（平成十五年法律第七十九号）第二十四条第一項に規定する緊急事態に相当するサイバーセキュリティに関する事象その他の情報通信ネットワーク又は電磁的記録媒体を通じた電子計算機に対する不正な活動から、国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるもの等を防御する能力の一層の強化を図るための施策について、幅広い観点から検討するものとする。
Article 3 Regarding cybersecurity incidents equivalent to the emergencies prescribed under Article 24, paragraph 1of the Law on the Peace and Independence of Japanand Maintenance of the Nation and the People's Security in Armed Attack Situations

etc. (Law No.79 of 2003), and other malicious activities against electronic computers through information and communications networks or electro-magnetic storage media, the Government shall examine, from a broad point of view, measures aimed at further strengthening the capability of the defense of infrastructure, which is the basis of citizen's living conditions and economic activities and the functional failure ordeterioration of which would risk enormous impacts to them.

（高度情報通信ネットワーク社会形成基本法の一部改正）

(Partial Revision of the Basic Act on the Formation of an Advanced Information and Telecommunications Network Society)

第四条　高度情報通信ネットワーク社会形成基本法の一部を次のように改正する。

第二十六条第一項中「事務」の下に「（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二十五条第一項に掲げる事務のうちサイバーセキュリティに関する施策で重要なものの実施の推進に関するものを除く。）」を加える。

Article 4 The Basic Act on the Formation of an Advanced Information and Telecommunications Network Society shall be partially revised by inserting the following afterthe "work" in Article 26, paragraph 1: "(excluding those functions related to the promotion of the implementation of important cybersecurity-related measures for thefunctions listed in Article 25, paragraph 1 of the Basic Act on Cybersecurity [Act No.104 of 2014])".

7. EC

2013/0027 (COD) LEX 1683 PE-CONS 26/16 TELECOM 122 DATAPROTECT 64 CYBER 71 MI 460 CSC 189 CODEC 904, DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL CONCERNING MEASURES FOR A HIGH COMMON LEVEL OF SECURITY OF NETWORK AND INFORMATION SYSTEMS ACROSS THE UNION, Strasbourg, 6 July 2016

(http://data.consilium.europa.eu/doc/document/PE-26-2016-INIT/en/pdf)

EUROPEAN UNION

THE EUROPEAN PARLIAMENT

THE COUNCIL

Strasbourg, 6 July 2016 (OR. en)

2013/0027 (COD) LEX 1683
PE-CONS 26/16

TELECOM 122
DATAPROTECT 64
CYBER 71
MI 460
CSC 189
CODEC 904

DIRECTIVE

OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL CONCERNING MEASURES FOR A HIGH COMMON LEVEL OF SECURITY OF NETWORK AND INFORMATION SYSTEMS ACROSS THE UNION

Directive (EU) 2016/... of the European Parliament and of the Council of 6 July 2016

concerning measures for a high common level of security of network and information systems across the Union

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee[1],

Acting in accordance with the ordinary legislative procedure[2],

---

[1] OJ C 271, 19.9.2013, p. 133.

[2] Position of the European Parliament of 13 March 2014 (not yet published in the Official Journal) and position of the Council at first reading of 17 May 2016 (not yet published in the Official Journal). Position of the European Parliament of 6 July 2016 (not yet published in the Official Journal).

Whereas:

(1) Network and information systems and services play a vital role in society. Their reliability and security are essential to economic and societal activities, and in particular to the functioning of the internal market.

(2) The magnitude, frequency and impact of security incidents are increasing, and represent a major threat to the functioning of network and information systems. Those systems may also become a target for deliberate harmful actions intended to damage or interrupt the operation of the systems. Such incidents can impede the pursuit of economic activities, generate substantial financial losses, undermine user confidence and cause major damage to the economy of the Union.

(3) Network and information systems, and primarily the internet, play an essential role in facilitating the cross–border movement of goods, services and people. Owing to that transnational nature, substantial disruptions of those systems, whether intentional or unintentional and regardless of where they occur, can affect individual Member States and the Union as a whole. The security of network and information systems is therefore essential for the smooth functioning of the internal market.

(4) Building upon the significant progress within the European Forum of Member States in fostering discussions and exchanges on good policy practices, including the development of principles for European cyber-crisis cooperation, a

Cooperation Group, composed of representatives of Member States, the Commission, and the European Union Agency for Network and Information Security ('ENISA'), should be established to support and facilitate strategic cooperation between the Member States regarding the security of network and information systems. For that group to be effective and inclusive, it is essential that all Member States have minimum capabilities and a strategy ensuring a high level of security of network and information systems in their territory. In addition, security and notification requirements should apply to operators of essential services and to digital service providers to promote a culture of risk management and ensure that the most serious incidents are reported.

(5) The existing capabilities are not sufficient to ensure a high level of security of network and information systems within the Union. Member States have very different levels of preparedness, which has led to fragmented approaches across the Union. This results in an unequal level of protection of consumers and businesses, and undermines the overall level of security of network and information systems within the Union. Lack of common requirements on operators of essential services and digital service providers in turn makes it impossible to set up a global and effective mechanism for cooperation at Union level. Universities and research centres have a decisive role to play in spurring research, development and innovation in those areas.

(6) Responding effectively to the challenges of the security of network and information systems therefore requires a global approach at Union level covering common minimum capacity building and planning requirements, exchange of information, cooperation and common security requirements for operators of essential services and digital service providers. However, operators of essential services and digital service providers are not precluded from implementing security measures that are stricter than those provided for under this Directive.

(7) To cover all relevant incidents and risks, this Directive should apply to both operators of essential services and digital service providers. However, the obligations on operators of essential services and digital service providers should not apply to undertakings providing public communication networks or publicly available electronic communication services within the meaning of Directive 2002/21/EC of the European Parliament and of the Council[1], which are subject to the specific security and integrity requirements laid down in that Directive, nor should they apply to trust service providers within the meaning of Regulation (EU) No 910/2014 of the European Parliament and of the Council[2], which are subject to the security requirements laid down in that Regulation.

[1] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) (OJ L 108, 24.4.2002, p. 33).

[2] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73).

(8) This Directive should be without prejudice to the possibility for each Member State to take the necessary measures to ensure the protection of the essential interests of its security, to safeguard public policy and public security, and to allow for the investigation, detection and prosecution of criminal offences. In accordance with Article 346 of the Treaty on the Functioning of the European Union (TFEU), no Member State is to be obliged to supply information the disclosure of which it considers to be contrary to the essential interests of its security. In this context, Council Decision 2013/488/EU[1] and non–disclosure agreements, or informal non–disclosure agreements such as the Traffic Light Protocol, are of relevance.

(9) Certain sectors of the economy are already regulated or may be regulated in the future by sector–specific Union legal acts that include rules related to the security of network and information systems. Whenever those Union legal acts contain provisions imposing requirements concerning the security of network and information systems or notifications of incidents, those provisions should apply if they contain requirements which are at least equivalent in effect to the obligations contained in this Directive. Member States should then apply the provisions of such sector–specific Union legal acts, including those relating to jurisdiction, and should not carry out the identification process for operators of essential services as defined by this Directive. In this context, Member States should provide information to the Commission on the application of such *lex specialis* provisions. In determining whether the requirements on the security of network and information systems and the notification of incidents contained in sector–specific Union legal acts are equivalent to those contained in this Directive, regard should only be had to the provisions of relevant Union legal acts and their application in the Member States.

---

1 Council Decision 2013/488/EU of 23 September 2013 on the security rules for protecting EU classified information (OJ L 274, 15.10.2013, p. 1).

(10) In the water transport sector, security requirements for companies, ships, port facilities, ports and vessel traffic services under Union legal acts cover all operations, including radio and telecommunication systems, computer systems and networks. Part of the mandatory procedures to be followed includes the reporting of all incidents and should therefore be considered as *lex specialis*, in so far as those requirements are at least equivalent to the corresponding provisions of this Directive.

(11) When identifying operators in the water transport sector, Member States should take into account existing and future international codes and guidelines developed in particular by the International Maritime Organisation, with a view to providing individual maritime operators with a coherent approach.

(12) Regulation and supervision in the sectors of banking and financial market infrastructures is highly harmonised at Union level, through the use of primary

and secondary Union law and standards developed together with the European supervisory authorities. Within the banking union, the application and the supervision of those requirements are ensured by the single supervisory mechanism. For Member States that are not part of the banking union, this is ensured by the relevant banking regulators of Member States. In other areas of financial sector regulation, the European System of Financial Supervision also ensures a high degree of commonality and convergence in supervisory practices. The European Securities Markets Authority also plays a direct supervision role for certain entities, namely credit-rating agencies and trade repositories.

(13) Operational risk is a crucial part of prudential regulation and supervision in the sectors of banking and financial market infrastructures. It covers all operations including the security, integrity and resilience of network and information systems. The requirements in respect of those systems, which often exceed the requirements provided for under this Directive, are set out in a number of Union legal acts, including: rules on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, and rules on prudential requirements for credit institutions and investment firms, which include requirements concerning operational risk; rules on markets in financial instruments, which include requirements concerning risk assessment for investment firms and for regulated markets; rules on OTC derivatives, central counterparties and trade repositories, which include requirements concerning operational risk for central counterparties and trade repositories; and rules on improving securities settlement in the Union and on central securities depositories, which include requirements concerning operational risk. Furthermore, requirements for notification of incidents are part of normal supervisory practice in the financial sector and are often included in supervisory manuals.

Member States should consider those rules and requirements in their application of *lex specialis*.

(14) As noted by the European Central Bank in its opinion of 25 July 2014[1], this Directive does not affect the regime under Union law for the Eurosystem's oversight of payment and settlement systems. It would be appropriate for the authorities responsible for such oversight to exchange experiences on matters concerning security of network and information systems with the competent authorities under this Directive. The same consideration applies to non–euro area members of the European System of Central Banks exercising such oversight of payment and settlement systems on the basis of national laws and regulations.

---

1 OJ C 352, 7.10.2014, p. 4.

(15) An online marketplace allows consumers and traders to conclude online sales or service contracts with traders, and is the final destination for the conclusion of those contracts. It should not cover online services that serve only as an intermediary to third–party services through which a contract can ultimately be concluded. It should therefore not cover online services that compare the price of particular products or services from different traders, and then redirect the user to the preferred trader to purchase the product. Computing services provided by the

online marketplace may include processing of transactions, aggregations of data or profiling of users. Application stores, which operate as online stores enabling the digital distribution of applications or software programmes from third parties, are to be understood as being a type of online marketplace.

(16) An online search engine allows the user to perform searches of, in principle, all websites on the basis of a query on any subject. It may alternatively be focused on websites in a particular language. The definition of an online search engine provided in this Directive should not cover search functions that are limited to the content of a specific website, irrespective of whether the search function is provided by an external search engine. Neither should it cover online services that compare the price of particular products or services from different traders, and then redirect the user to the preferred trader to purchase the product.

(17) Cloud computing services span a wide range of activities that can be delivered according to different models. For the purposes of this Directive, the term 'cloud computing services' covers services that allow access to a scalable and elastic pool of shareable computing resources. Those computing resources include resources such as networks, servers or other infrastructure, storage, applications and services. The term 'scalable' refers to computing resources that are flexibly allocated by the cloud service provider, irrespective of the geographical location of the resources, in order to handle fluctuations in demand. The term 'elastic pool' is used to describe those computing resources that are provisioned and released according to demand in order to rapidly increase and decrease resources available depending on workload. The term 'shareable' is used to describe those computing resources that are provided to multiple users who share a common access to the service, but where the processing is carried out separately for each user, although the service is provided from the same electronic equipment.

(18) The function of an internet exchange point (IXP) is to interconnect networks. An IXP does not provide network access or act as a transit provider or carrier. Nor does an IXP provide other services unrelated to interconnection, although this does not preclude an IXP operator from providing unrelated services. An IXP exists to interconnect networks that are technically and organisationally separate. The term 'autonomous system' is used to describe a technically stand–alone network.

(19) Member States should be responsible for determining which entities meet the criteria of the definition of operator of essential services. In order to ensure a consistent approach, the definition of operator of essential services should be coherently applied by all

Member States. To that end, this Directive provides for the assessment of the entities active in specific sectors and subsectors, the establishment of a list of essential services, the consideration of a common list of cross–sectoral factors to determine whether a potential incident would have a significant disruptive effect, a consultation process involving relevant Member States in the case of entities providing services in more than one

Member State, and the support of the Cooperation Group in the identification process. In order to ensure that possible changes in the market are accurately reflected, the list of identified operators should be reviewed regularly by Member States and updated when necessary. Finally, Member States should

submit to the Commission the information necessary to assess the extent to which this common methodology has allowed a consistent application of the definition by Member States.

(20) In the process of identification of operators of essential services, Member States should assess, at least for each subsector referred to in this Directive, which services have to be considered as essential for the maintenance of critical societal and economic activities, and whether the entities listed in the sectors and subsectors referred to in this Directive and providing those services meet the criteria for the identification of operators. When assessing whether an entity provides a service which is essential for the maintenance of critical societal or economic activities, it is sufficient to examine whether that entity provides a service that is included in the list of essential services. Furthermore, it should be demonstrated that provision of the essential service is dependent on network and information systems. Finally, when assessing whether an incident would have a significant disruptive effect on the provision of the service, Member States should take into account a number of cross–sectoral factors, as well as, where appropriate, sector–specific factors.

(21) For the purposes of identifying operators of essential services, establishment in a Member State implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary possessing legal personality, is not the determining factor in this respect.

(22) It is possible that entities operating in the sectors and subsectors referred to in this Directive provide both essential and non–essential services. For example, in the air transport sector, airports provide services which might be considered by a Member State to be essential, such as the management of the runways, but also a number of services which might be considered as non–essential, such as the provision of shopping areas. Operators of essential services should be subject to the specific security requirements only with respect to those services which are deemed to be essential. For the purpose of identifying operators, Member States should therefore establish a list of the services which are considered as essential.

(23) The list of services should contain all services provided in the territory of a given Member State that fulfil the requirements under this Directive. Member States should be able to supplement the existing list by including new services. The list of services should serve as a reference point for Member States, allowing for identification of operators of essential services. Its purpose is to identify the types of essential services in any given sector referred to in this Directive, thus distinguishing them from non–essential activities for which an entity active in any given sector might be responsible. The list of services established by each Member State would serve as further input in the assessment of the regulatory practice of each Member State with a view to ensuring the overall level of consistency of the identification process amongst Member States.

(24) For the purposes of the identification process, where an entity provides an essential service in two or more Member States, those Member States should

engage in bilateral or multilateral discussions with each other. This consultation process is intended to help them to assess the critical nature of the operator in terms of cross–border impact, thereby allowing each Member State involved to present its views regarding the risks associated with the services provided. The Member States concerned should take into account each other's views in this process, and should be able to request the assistance of the Cooperation Group in this regard.

(25) As a result of the identification process, Member States should adopt national measures to determine which entities are subject to obligations regarding the security of network and information systems. This result could be achieved by adopting a list enumerating all operators of essential services or by adopting national measures including objective quantifiable criteria, such as the output of the operator or the number of users, which make it possible to determine which entities are subject to obligations regarding the security of network and information systems. The national measures, whether already existing or adopted in the context of this Directive, should include all legal measures, administrative measures and policies allowing for the identification of operators of essential services under this Directive.

(26) In order to give an indication of the importance, in relation to the sector concerned, of the identified operators of essential services, Member States should take into account the number and the size of those operators, for example in terms of market share or of the quantity produced or carried, without being obliged to divulge information which would reveal which operators have been identified.

(27) In order to determine whether an incident would have a significant disruptive effect on the provision of an essential service, Member States should take into account a number of different factors, such as the number of users relying on that service for private or professional purposes. The use of that service can be direct, indirect or by intermediation. When assessing the impact that an incident could have, in terms of its degree and duration, on economic and societal activities or public safety, Member States should also assess the time likely to elapse before the discontinuity would start to have a negative impact.

(28) In addition to the cross–sectoral factors, sector–specific factors should also be considered in order to determine whether an incident would have a significant disruptive effect on the provision of an essential service. With regard to energy suppliers, such factors could include the volume or proportion of national power generated; for oil suppliers, the volume per day; for air transport, including airports and air carriers, rail transport and maritime ports, the proportion of national traffic volume and the number of passengers or cargo operations per year; for banking or financial market infrastructures, their systemic importance based on total assets or the ratio of those total assets to GDP; for the health sector, the number of patients under the provider's care per year; for water production, processing and supply, the volume and number and types of users supplied, including, for example, hospitals, public service organisations, or individuals, and the existence of alternative sources of water to cover the same geographical area.

(29) To achieve and maintain a high level of security of network and information systems, each Member State should have a national strategy on the security of network and information systems defining the strategic objectives and concrete policy actions to be implemented.

(30) In view of the differences in national governance structures and in order to safeguard already existing sectoral arrangements or Union supervisory and regulatory bodies, and to avoid duplication, Member States should be able to designate more than one national competent authority responsible for fulfilling the tasks linked to the security of the network and information systems of operators of essential services and digital service providers under this Directive.

(31) In order to facilitate cross–border cooperation and communication and to enable this Directive to be implemented effectively, it is necessary for each Member State, without prejudice to sectoral regulatory arrangements, to designate a national single point of contact responsible for coordinating issues related to the security of network and information systems and cross–border cooperation at Union level. Competent authorities and single points of contact should have the adequate technical, financial and human resources to ensure that they can carry out the tasks assigned to them in an effective and efficient manner and thus achieve the objectives of this Directive. As this Directive aims to improve the functioning of the internal market by creating trust and confidence,
Member State bodies need to be able to cooperate effectively with economic actors and to be structured accordingly.

(32) Competent authorities or the computer security incident response teams ('CSIRTs') should receive notifications of incidents. The single points of contact should not receive directly any notifications of incidents unless they also act as a competent authority or a CSIRT. A competent authority or a CSIRT should however be able to task the single point of contact with forwarding incident notifications to the single points of contact of other affected Member States.

(33) To ensure the effective provision of information to the Member States and to the Commission, a summary report should be submitted by the single point of contact to the Cooperation Group, and should be anonymised in order to preserve the confidentiality of the notifications and the identity of operators of essential services and digital service providers, as information on the identity of the notifying entities is not required for the exchange of best practice in the Cooperation Group. The summary report should include information on the number of notifications received, as well as an indication of the nature of the notified incidents, such as the types of security breaches, their seriousness or their duration.

(34) Member States should be adequately equipped, in terms of both technical and organisational capabilities, to prevent, detect, respond to and mitigate network and information system incidents and risks. Member States should therefore ensure that they have well–functioning CSIRTs, also known as computer emergency response teams ('CERTs'), complying with essential requirements to guarantee effective and compatible capabilities to deal with incidents and risks and ensure efficient cooperation at Union level. In order for all types of operators of essential

services and digital service providers to benefit from such capabilities and cooperation, Member States should ensure that all types are covered by a designated CSIRT. Given the importance of international cooperation on cybersecurity, CSIRTs should be able to participate in international cooperation networks in addition to the CSIRTs network established by this Directive.

(35) As most network and information systems are privately operated, cooperation between the public and private sectors is essential. Operators of essential services and digital service providers should be encouraged to pursue their own informal cooperation mechanisms to ensure the security of network and information systems. The Cooperation Group should be able to invite relevant stakeholders to the discussions where appropriate. To encourage effectively the sharing of information and of best practice, it is essential to ensure that operators of essential services and digital service providers who participate in such exchanges are not disadvantaged as a result of their cooperation.

(36) ENISA should assist the Member States and the Commission by providing expertise and advice and by facilitating the exchange of best practice. In particular, in the application of this Directive, the Commission should, and Member States should be able to, consult ENISA. To build capacity and knowledge among Member States, the Cooperation Group should also serve as an instrument for the exchange of best practice, discussion of capabilities and preparedness of the Member States and, on a voluntary basis, to assist its members in evaluating national strategies on the security of network and information systems, building capacity and evaluating exercises relating to the security of network and information systems.

(37) Where appropriate, Member States should be able to use or adapt existing organisational structures or strategies when applying this Directive.

(38) The respective tasks of the Cooperation Group and of ENISA are interdependent and complementary. In general, ENISA should assist the Cooperation Group in the execution of its tasks, in line with the objective of ENISA set out in Regulation (EU) No 526/2013 of the European Parliament and the Council[1], namely to assist the Union institutions, bodies, offices and agencies and the Member States in implementing the policies necessary to meet the legal and regulatory requirements of network and information system security under existing and future legal acts of the Union. In particular, ENISA should provide assistance

in those areas that correspond to its own tasks, as set out in Regulation (EU) No 526/2013, namely analysing network and information system security strategies, supporting the organisation and running of Union exercises relating to the security of network and information systems, and exchanging information and best practice on awareness–raising and training. ENISA should also be involved in the development of guidelines for

sector-specific criteria for determining the significance of the impact of an incident.

(39) In order to promote advanced security of network and information systems, the Cooperation Group should, where appropriate, cooperate with relevant Union

institutions, bodies, offices and agencies, to exchange know–how and best practice, and to provide advice on security aspects of network and information systems that might have an impact on their work, while respecting existing arrangements for the exchange of restricted information. In cooperating with law enforcement authorities regarding the security aspects of network and information systems that might have an impact on their work, the Cooperation Group should respect existing channels of information and established networks.

---

1 Regulation (EU) No 526/2013 of the European Parliament and the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 (OJ L 165, 18.6.2013, p. 41).

(40) Information about incidents is increasingly valuable to the general public and businesses, particularly small and medium–sized enterprises. In some cases, such information is already provided via websites at the national level, in the language of a specific country and focusing mainly on incidents and occurrences with a national dimension. Given that businesses increasingly operate across borders and citizens use online services, information on incidents should be provided in an aggregated form at Union level. The secretariat of the CSIRTs network is encouraged to maintain a website or to host a dedicated page on an existing website, where general information on major incidents that have occurred across the Union is made available to the general public, with a specific focus on the interests and needs of businesses. CSIRTs participating in the CSIRTs network are encouraged to provide on a voluntary basis the information to be published on that website, without including confidential or sensitive information.

(41) Where information is considered to be confidential in accordance with Union and national rules on business confidentiality, such confidentiality should be ensured when carrying out the activities and fulfilling the objectives set by this Directive.

(42) Exercises which simulate real–time incident scenarios are essential for testing Member States' preparedness and cooperation regarding the security of network and information systems. The CyberEurope cycle of exercises coordinated by ENISA with the participation of the Member States is a useful tool for testing and drawing up recommendations on how incident-handling at Union level should improve over time. Considering that the Member States are not currently under any obligation to either plan or participate in exercises, the creation of the CSIRTs network under this Directive should enable Member States to participate in exercises on the basis of accurate planning and strategic choices. The Cooperation Group set up under this Directive should discuss the strategic decisions regarding exercises, in particular but not exclusively as regards the regularity of the exercises and the design of the scenarios. ENISA should, in accordance with its mandate, support the organisation and running of Union–wide exercises by providing its expertise and advice to the Cooperation Group and the CSIRTs network.

(43) Given the global nature of security problems affecting network and information

systems, there is a need for closer international cooperation to improve security standards and information exchange, and to promote a common global approach to security issues.

(44) Responsibilities in ensuring the security of network and information systems lie, to a great extent, with operators of essential services and digital service providers. A culture of risk management, involving risk assessment and the implementation of security measures appropriate to the risks faced, should be promoted and developed through appropriate regulatory requirements and voluntary industry practices. Establishing a trustworthy level playing–field is also essential to the effective functioning of the Cooperation Group and the CSIRTs network, to ensure effective cooperation from all Member States.

(45) This Directive applies only to those public administrations which are identified as operators of essential services. Therefore, it is the responsibility of Member States to ensure the security of network and information systems of public administrations not falling within the scope of this Directive.

(46) Risk–management measures include measures to identify any risks of incidents, to prevent, detect and handle incidents and to mitigate their impact. The security of network and information systems comprises the security of stored, transmitted and processed data.

(47) Competent authorities should retain the ability to adopt national guidelines concerning the circumstances in which operators of essential services are required to notify incidents.

(48) Many businesses in the Union rely on digital service providers for the provision of their services. As some digital services could be an important resource for their users, including operators of essential services, and as such users might not always have alternatives available, this Directive should also apply to providers of such services. The security, continuity and reliability of the type of digital services referred to in this Directive are of the essence for the smooth functioning of many businesses. A disruption of such a digital service could prevent the provision of other services which rely on it and could thus have an impact on key economic and societal activities in the Union. Such digital services might therefore be of crucial importance for the smooth functioning of businesses that depend on them and, moreover, for the participation of such businesses in the internal market and cross–border trade across the Union. Those digital service providers that are subject to this Directive are those that are considered to offer digital services on which many businesses in the Union increasingly rely.

(49) Digital service providers should ensure a level of security commensurate with the degree of risk posed to the security of the digital services they provide, given the importance of their services to the operations of other businesses within the Union. In practice, the degree of risk for operators of essential services, which are often essential for the maintenance of critical societal and economic activities, is higher than for digital service providers. Therefore, the security requirements for digital service providers should be lighter. Digital service providers should remain free to

take measures they consider appropriate to manage the risks posed to the security of their network and information systems. Because of their cross–border nature, digital service providers should be subject to a more harmonised approach at Union level. Implementing acts should facilitate the specification and implementation of such measures.

(50) While hardware manufacturers and software developers are not operators of essential services, nor are they digital service providers, their products enhance the security of network and information systems. Therefore, they play an important role in enabling operators of essential services and digital service providers to secure their network and information systems. Such hardware and software products are already subject to existing rules on product liability.

(51) Technical and organisational measures imposed on operators of essential services and digital service providers should not require a particular commercial information and communications technology product to be designed, developed or manufactured in a particular manner.

(52) Operators of essential services and digital service providers should ensure the security of the network and information systems which they use. These are primarily private network and information systems managed by their internal IT staff or the security of which has been outsourced. The security and notification requirements should apply to the relevant operators of essential services and digital service providers regardless of whether they perform the maintenance of their network and information systems internally or outsource it.

(53) To avoid imposing a disproportionate financial and administrative burden on operators of essential services and digital service providers, the requirements should be proportionate to the risk presented by the network and information system concerned, taking into account the state of the art of such measures. In the case of digital service providers, those requirements should not apply to micro– and small enterprises.

(54) Where public administrations in Member States use services offered by digital service providers, in particular cloud computing services, they might wish to require from the providers of such services additional security measures beyond what digital service providers would normally offer in compliance with the requirements of this Directive. They should be able to do so by means of contractual obligations.

(55) The definitions of online marketplaces, online search engines and cloud computing services in this Directive are for the specific purpose of this Directive, and without prejudice to any other instruments.

(56) This Directive should not preclude Member States from adopting national measures requiring public–sector bodies to ensure specific security requirements when they contract cloud computing services. Any such national measures should apply to the public–sector body concerned and not to the cloud computing service provider.

(57) Given the fundamental differences between operators of essential services, in particular their direct link with physical infrastructure, and digital service providers, in particular their cross–border nature, this Directive should take a differentiated approach with respect to the level of harmonisation in relation to those two groups of entities. For operators of essential services, Member States should be able to identify the relevant operators and impose stricter requirements than those laid down in this Directive. Member States should not identify digital service providers, as this Directive should apply to all digital service providers within its scope. In addition, this Directive and the implementing acts adopted under it should ensure a high level of harmonisation for digital service providers with respect to security and notification requirements. This should enable digital service providers to be treated in a uniform way across the Union, in a manner proportionate to their nature and the degree of risk which they might face.

(58) This Directive should not preclude Member States from imposing security and notification requirements on entities that are not digital service providers within the scope of this Directive, without prejudice to Member States' obligations under Union law.

(59) Competent authorities should pay due attention to preserving informal and trusted channels of information–sharing. Publicity of incidents reported to the competent authorities should duly balance the interest of the public in being informed about threats against possible reputational and commercial damage for the operators of essential services and digital service providers reporting incidents. In the implementation of the notification obligations, competent authorities and the CSIRTs should pay particular attention to the need to keep information about product vulnerabilities strictly confidential, prior to the release of appropriate security fixes.

(60) Digital service providers should be subject to light–touch and reactive *ex post* supervisory activities justified by the nature of their services and operations. The competent authority concerned should therefore only take action when provided with evidence, for example by the digital service provider itself, by another competent authority, including a competent authority of another Member State, or by a user of the service, that a digital service provider is not complying with the requirements of this Directive, in particular following the occurrence of an incident. The competent authority should therefore have no general obligation to supervise digital service providers.

(61) Competent authorities should have the necessary means to perform their duties, including powers to obtain sufficient information in order to assess the level of security of network and information systems.

(62) Incidents may be the result of criminal activities the prevention, investigation and prosecution of which is supported by coordination and cooperation between operators of essential services, digital service providers, competent authorities and law enforcement authorities. Where it is suspected that an incident is related to serious criminal activities under Union or national law, Member States should encourage operators of essential services and digital service providers to report incidents of a suspected serious criminal nature to the relevant law

enforcement authorities. Where appropriate, it is desirable that coordination between competent authorities and law enforcement authorities of different Member States be facilitated by the European Cybercrime Centre (EC3) and ENISA.

(63) Personal data are in many cases compromised as a result of incidents. In this context, competent authorities and data protection authorities should cooperate and exchange information on all relevant matters to tackle any personal data breaches resulting from incidents.

(64) Jurisdiction in respect of digital service providers should be attributed to the Member State in which the digital service provider concerned has its main establishment in the Union, which in principle corresponds to the place where the provider has its head office in the Union. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in this respect. This criterion should not depend on whether the network and information systems are physically located in a given place; the presence and use of such systems do not, in themselves, constitute such main establishment and are therefore not criteria for determining the main establishment.

(65) Where a digital service provider not established in the Union offers services within the Union, it should designate a representative. In order to determine whether such a digital service provider is offering services within the Union, it should be ascertained whether it is apparent that the digital service provider is planning to offer services to persons in one or more Member States. The mere accessibility in the Union of the digital service provider's or an intermediary's website or of an email address and of other contact details, or the use of a language generally used in the third country where the digital service provider is established, is insufficient to ascertain such an intention. However, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the digital service provider is planning to offer services within the Union. The representative should act on behalf of the digital service provider and it should be possible for competent authorities or the CSIRTs to contact the representative. The representative should be explicitly designated by a written mandate of the digital service provider to act on the latter's behalf with regard to the latter's obligations under this Directive, including incident reporting.

(66) Standardisation of security requirements is a market–driven process. To ensure a convergent application of security standards, Member States should encourage compliance or conformity with specified standards so as to ensure a high level of security of network and information systems at Union level. ENISA should assist Member States through advice and guidelines. To this end, it might be helpful to draft harmonised standards, which should be done in accordance with Regulation (EU) No 1025/2012 of the

European Parliament and of the Council[1].

(67) Entities falling outside the scope of this Directive may experience incidents having a significant impact on the services they provide. Where those entities consider that it is in the public interest to notify the occurrence of such incidents, they should be able to do so on a voluntary basis. Such notifications should be processed by the competent authority or the CSIRT where such processing does not constitute a disproportionate or undue burden on the Member States concerned.

---

1 Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council (OJ L 316, 14.11.2012, p. 12).

(68) In order to ensure uniform conditions for the implementation of this Directive, implementing powers should be conferred on the Commission to lay down the procedural arrangements necessary for the functioning of the Cooperation Group and the security and notification requirements applicable to digital service providers. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council**1**. When adopting implementing acts related to the procedural arrangements necessary for the functioning of the Cooperation Group, the Commission should take the utmost account of the opinion of ENISA.

(69) When adopting implementing acts on the security requirements for digital service providers, the Commission should take the utmost account of the opinion of ENISA and should consult interested stakeholders. Moreover, the Commission is encouraged to take into account the following examples: as regards security of systems and facilities: physical and environmental security, security of supplies, access control to network and information systems and integrity of network and information systems; as regards incident handling: incident-handling procedures, incident detection capability, incident reporting and communication; as regards business continuity management: service continuity strategy and contingency plans, disaster recovery capabilities; and as regards monitoring, auditing and testing: monitoring and logging policies, exercise contingency plans, network and information systems testing, security assessments and compliance monitoring.

[1] Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

(70) In the implementation of this Directive, the Commission should liaise as appropriate with relevant sectoral committees and relevant bodies set up at Union level in the fields covered by this Directive.

(71) The Commission should periodically review this Directive, in consultation with interested stakeholders, in particular with a view to determining the need for modification in the light of changes to societal, political, technological or market conditions.

(72) The sharing of information on risks and incidents within the Cooperation Group and the CSIRTs network and the compliance with the requirements to notify incidents to the national competent authorities or the CSIRTs might require processing of personal data. Such processing should comply with Directive 95/46/EC of the European Parliament and the Council[1] and Regulation (EC) No 45/2001 of the European Parliament and of the Council[2]. In the application of this Directive, Regulation (EC) No 1049/2001 of the European Parliament and of the Council[3] should apply as appropriate.

(73) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on 14 June 2013[4].

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

[2] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of

such data
(OJ L 8, 12.1.2001, p. 1).

[3] Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43).

[4] OJ C 32, 4.2.2014, p. 19.

(74) Since the objective of this Directive, namely to achieve a high common level of security of network and information systems in the Union, cannot be sufficiently achieved by the Member States but can rather, by reason of the effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Directive does not go beyond what is necessary in order to achieve that objective.

(75) This Directive respects the fundamental rights, and observes the principles, recognised by the Charter of Fundamental Rights of the European Union, in particular the right to respect for private life and communications, the protection of personal data, the freedom to conduct a business, the right to property, the right to an effective remedy before a court and the right to be heard. This Directive should be implemented in accordance with those rights and principles,

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I GENERAL PROVISIONS

Article 1

Subject matter and scope

1. This Directive lays down measures with a view to achieving a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market.

2. To that end, this Directive:

(a) lays down obligations for all Member States to adopt a national strategy on the security of network and information systems;

(b) creates a Cooperation Group in order to support and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence amongst them;

(c) creates a computer security incident response teams network ('CSIRTs network') in order to contribute to the development of trust and confidence between
Member States and to promote swift and effective operational cooperation;

(d) establishes security and notification requirements for operators of essential services and for digital service providers;

(e) lays down obligations for Member States to designate national competent authorities, single points of contact and CSIRTs with tasks related to the security of network and information systems.

3. The security and notification requirements provided for in this Directive shall not apply to undertakings which are subject to the requirements of Articles 13a and 13b of
Directive 2002/21/EC, or to trust service providers which are subject to the requirements of Article 19 of Regulation (EU) No 910/2014.

4. This Directive applies without prejudice to Council Directive 2008/114/EC[1] and Directives 2011/93/EU[2] and 2013/40/EU[3] of the European Parliament and of the Council.

5. Without prejudice to Article 346 TFEU, information that is confidential pursuant to Union and national rules, such as rules on business confidentiality, shall be exchanged with the Commission and other relevant authorities only where such exchange is necessary for the application of this Directive. The information exchanged shall be limited to that which is relevant and proportionate to the purpose of such exchange. Such exchange of information shall preserve the confidentiality of that information and protect the security and commercial interests of operators of essential services and digital service providers.

---

[1] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (OJ L 345, 23.12.2008, p. 75).

[2] Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ L 335, 17.12.2011, p. 1).

[3] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (OJ L 218, 14.8.2013, p. 8).

6. This Directive is without prejudice to the actions taken by Member States to safeguard their essential State functions, in particular to safeguard national security, including actions protecting information the disclosure of which Member States consider contrary to the essential interests of their security, and to maintain law and order, in particular to allow for the investigation, detection and prosecution of criminal offences.

7. Where a sector–specific Union legal act requires operators of essential services or digital service providers either to ensure the security of their network and information systems or to notify incidents, provided that such requirements are at

least equivalent in effect to the obligations laid down in this Directive, those provisions of that sector–specific Union legal act shall apply.

Article 2 Processing of personal data

1. Processing of personal data pursuant to this Directive shall be carried out in accordance with Directive 95/46/EC.

2. Processing of personal data by Union institutions and bodies pursuant to this Directive shall be carried out in accordance with Regulation (EC) No 45/2001.

Article 3 Minimum harmonisation

Without prejudice to Article 16(10) and to their obligations under Union law, Member States may adopt or maintain provisions with a view to achieving a higher level of security of network and information systems.

Article 4. Defnitions

For the purposes of this Directive, the following definitions apply:

(1) 'network and information system' means:

(a) an electronic communications network within the meaning of point (a) of Article 2 of Directive 2002/21/EC;

(b) any device or group of inter–connected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data; or

(c) digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance;

(2) 'security of network and information systems' means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems;

(3) 'national strategy on the security of network and information systems' means a framework providing strategic objectives and priorities on the security of network and information systems at national level;

(4) 'operator of essential services' means a public or private entity of a type referred to in Annex II, which meets the criteria laid down in Article 5(2);

(5) 'digital service' means a service within the meaning of point (b) of Article 1(1)

of Directive (EU) 2015/1535 of the European Parliament and of the Council[1] which is of a type listed in Annex III;

(6) 'digital service provider' means any legal person that provides a digital service;

(7) 'incident' means any event having an actual adverse effect on the security of network and information systems;

(8) 'incident handling' means all procedures supporting the detection, analysis and containment of an incident and the response thereto;

---

[1] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1).

(9) 'risk' means any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems;

(10) 'representative' means any natural or legal person established in the Union explicitly designated to act on behalf of a digital service provider not established in the Union, which may be addressed by a national competent authority or a CSIRT instead of the digital service provider with regard to the obligations of that digital service provider under this Directive;

(11) 'standard' means a standard within the meaning of point (1) of Article 2 of Regulation (EU) No 1025/2012;

(12) 'specification' means a technical specification within the meaning of point (4) of Article 2 of Regulation (EU) No 1025/2012;

(13) 'internet exchange point (IXP)' means a network facility which enables the interconnection of more than two independent autonomous systems, primarily for the purpose of facilitating the exchange of internet traffic; an IXP provides interconnection only for autonomous systems; an IXP does not require the internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system, nor does it alter or otherwise interfere with such traffic;

(14) 'domain name system (DNS)' means a hierarchical distributed naming system in a network which refers queries for domain names;

(15) 'DNS service provider' means an entity which provides DNS services on the internet;

(16) 'top–level domain name registry' means an entity which administers and operates the registration of internet domain names under a specific top–level

domain (TLD);

(17) ‘online marketplace’ means a digital service that allows consumers and/or traders as respectively defined in point (a) and in point (b) of Article 4(1) of Directive 2013/11/EU of the European Parliament and of the Council[1] to conclude online sales or service contracts with traders either on the online marketplace’s website or on a trader’s website that uses computing services provided by the online marketplace;

(18) ‘online search engine’ means a digital service that allows users to perform searches of, in principle, all websites or websites in a particular language on the basis of a query on any subject in the form of a keyword, phrase or other input, and returns links in which information related to the requested content can be found;

(19) ‘cloud computing service’ means a digital service that enables access to a scalable and elastic pool of shareable computing resources.

Article 5
Identification of operators of essential services

1. By … [27 months after the date of entry into force of this Directive], for each sector and subsector referred to in Annex II, Member States shall identify the operators of essential services with an establishment on their territory.

---

1 Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Directive on consumer ADR) (OJ L 165, 18.6.2013, p. 63).

2. The criteria for the identification of the operators of essential services, as referred to in point (4) of Article 4, shall be as follows:

(a) an entity provides a service which is essential for the maintenance of critical societal and/or economic activities;

(b) the provision of that service depends on network and information systems; and

(c) an incident would have significant disruptive effects on the provision of that service.

3. For the purposes of paragraph 1, each Member State shall establish a list of the services referred to in point (a) of paragraph 2.

4. For the purposes of paragraph 1, where an entity provides a service as referred to in point

(a) of paragraph 2 in two or more Member States, those Member States shall engage in consultation with each other. That consultation shall take place before a decision on identification is taken.

5. Member States shall, on a regular basis, and at least every two years after … [21 months after the entry into force of this Directive], review and, where appropriate, update the list of identified operators of essential services.

6. The role of the Cooperation Group shall be, in accordance with the tasks referred to in Article 11, to support Member States in taking a consistent approach in the process of identification of operators of essential services.

7. For the purpose of the review referred to in Article 23 and by … [27 months after the date of entry into force of this Directive], and every two years thereafter, Member States shall submit to the Commission the information necessary to enable the Commission to assess the implementation of this Directive, in particular the consistency of Member States' approaches to the identification of operators of essential services. That information shall include at least:

(a) national measures allowing for the identification of operators of essential services;

(b) the list of services referred to in paragraph 3;

(c) the number of operators of essential services identified for each sector referred to in Annex II and an indication of their importance in relation to that sector;

(d) thresholds, where they exist, to determine the relevant supply level by reference to the number of users relying on that service as referred to in point (a) of Article 6(1) or to the importance of that particular operator of essential services as referred to in point (f) of Article 6(1).

In order to contribute to the provision of comparable information, the Commission, taking the utmost account of the opinion of ENISA, may adopt appropriate technical guidelines on parameters for the information referred to in this paragraph.

Article 6 Significant disruptive effect

1. When determining the significance of a disruptive effect as referred to in point (c) of Article 5(2), Member States shall take into account at least the following cross–sectoral factors:

(a) the number of users relying on the service provided by the entity concerned;

(b) the dependency of other sectors referred to in Annex II on the service provided by that entity;

(c) the impact that incidents could have, in terms of degree and duration, on economic and societal activities or public safety;

(d) the market share of that entity;

(e) the geographic spread with regard to the area that could be affected by an incident;

(f) the importance of the entity for maintaining a sufficient level of the service, taking into account the availability of alternative means for the provision of that service.

2. In order to determine whether an incident would have a significant disruptive effect, Member States shall also, where appropriate, take into account sector–specific factors.

CHAPTER II

NATIONAL FRAMEWORKS ON THE SECURITY OF NETWORK AND INFORMATION SYSTEMS

Article 7

National strategy on the security of network and information systems

1. Each Member State shall adopt a national strategy on the security of network and information systems defining the strategic objectives and appropriate policy and regulatory measures with a view to achieving and maintaining a high level of security of network and information systems and covering at least the sectors referred to in Annex II and the services referred to in Annex III. The national strategy on the security of network and information systems shall address, in particular, the following issues:

(a) the objectives and priorities of the national strategy on the security of network and information systems;

(b) a governance framework to achieve the objectives and priorities of the national strategy on the security of network and information systems, including roles and responsibilities of the government bodies and the other relevant actors;

(c) the identification of measures relating to preparedness, response and

recovery, including cooperation between the public and private sectors;

(d) an indication of the education, awareness–raising and training programmes relating to the national strategy on the security of network and information systems;

(e) an indication of the research and development plans relating to the national strategy on the security of network and information systems;

(f) a risk assessment plan to identify risks;

(g) a list of the various actors involved in the implementation of the national strategy on the security of network and information systems.

2. Member States may request the assistance of ENISA in developing national strategies on the security of network and information systems.

3. Member States shall communicate their national strategies on the security of network and information systems to the Commission within three months from their adoption. In so doing, Member States may exclude elements of the strategy which relate to national security.

Article 8
National competent authorities and single point of contact

1. Each Member State shall designate one or more national competent authorities on the security of network and information systems ('competent authority'), covering at least the sectors referred to in Annex II and the services referred to in Annex III. Member States may assign this role to an existing authority or authorities.

2. The competent authorities shall monitor the application of this Directive at national level.

3. Each Member State shall designate a national single point of contact on the security of network and information systems ('single point of contact'). Member States may assign this role to an existing authority. Where a Member State designates only one competent authority, that competent authority shall also be the single point of contact.

4. The single point of contact shall exercise a liaison function to ensure cross–border cooperation of Member State authorities and with the relevant authorities in other Member States and with the Cooperation Group referred to in Article 11 and the CSIRTs network referred to in Article 12.

5. Member States shall ensure that the competent authorities and the single points of contact have adequate resources to carry out, in an effective and efficient manner,

the tasks assigned to them and thereby to fulfil the objectives of this Directive. Member States shall ensure effective, efficient and secure cooperation of the designated representatives in the Cooperation Group.

6. The competent authorities and single point of contact shall, whenever appropriate and in accordance with national law, consult and cooperate with the relevant national law enforcement authorities and national data protection authorities.

7. Each Member State shall notify to the Commission without delay the designation of the competent authority and single point of contact, their tasks, and any subsequent change thereto. Each Member State shall make public its designation of the competent authority and single point of contact. The Commission shall publish the list of designated single points of contacts.

Artiicle 9. Computer security incident response teams (CSIRTs)

1. Each Member State shall designate one or more CSIRTs which shall comply with the requirements set out in point (1) of Annex I, covering at least the sectors referred to in Annex II and the services referred to in Annex III, responsible for risk and incident handling in accordance with a well–defined process. A CSIRT may be established within a competent authority.

2. Member States shall ensure that the CSIRTs have adequate resources to effectively carry out their tasks as set out in point (2) of Annex I.

Member States shall ensure the effective, efficient and secure cooperation of their CSIRTs in the CSIRTs network referred to in Article 12.

3. Member States shall ensure that their CSIRTs have access to an appropriate, secure, and resilient communication and information infrastructure at national level.

4. Member States shall inform the Commission about the remit, as well as the main elements of the incident-handling process, of their CSIRTs.

5. Member States may request the assistance of ENISA in developing national CSIRTs.

Article 10. Cooperation at national level

1. Where they are separate, the competent authority, the single point of contact and the CSIRT of the same Member State shall cooperate with regard to the fulfilment of the obligations laid down in this Directive.

2. Member States shall ensure that either the competent authorities or the CSIRTs receive incident notifications submitted pursuant to this Directive. Where a Member State decides that CSIRTs shall not receive notifications, the CSIRTs shall, to the extent necessary to fulfil their tasks, be granted access to data on

incidents notified by operators of essential services, pursuant to Article 14(3) and (5), or by digital service providers, pursuant to Article 16(3) and (6).

3. Member States shall ensure that the competent authorities or the CSIRTs inform the single points of contact about incident notifications submitted pursuant to this Directive.

By … [24 months after the date of entry into force of this Directive], and every year thereafter, the single point of contact shall submit a summary report to the Cooperation Group on the notifications received, including the number of notifications and the nature of notified incidents, and the actions taken in accordance with Article 14(3) and (5) and Article 16(3) and (6).

CHAPTER III COOPERATION

Article 11 Cooperation Group

1. In order to support and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence, and with a view to achieving a high common level of security of network and information systems in the Union, a Cooperation Group is hereby established.

The Cooperation Group shall carry out its tasks on the basis of biennial work programmes as referred to in the second subparagraph of paragraph 3.

2. The Cooperation Group shall be composed of representatives of the Member States, the Commission and ENISA.

Where appropriate, the Cooperation Group may invite representatives of the relevant stakeholders to participate in its work.

The Commission shall provide the secretariat.

3. The Cooperation Group shall have the following tasks:

(a) providing strategic guidance for the activities of the CSIRTs network established under Article 12;

(b) exchanging best practice on the exchange of information related to incident notification as referred to in Article 14(3) and (5) and Article 16(3) and (6);

(c) exchanging best practice between Member States and, in collaboration with ENISA, assisting Member States in building capacity to ensure the security of network and information systems;

(d) discussing capabilities and preparedness of the Member States, and, on a

voluntary basis, evaluating national strategies on the security of network and information systems and the effectiveness of CSIRTs, and identifying best practice;

(e) exchanging information and best practice on awareness-raising and training;

(f) exchanging information and best practice on research and development relating to the security of network and information systems;

(g) where relevant, exchanging experiences on matters concerning the security of network and information systems with relevant Union institutions, bodies, offices and agencies;

(h) discussing the standards and specifications referred to in Article 19 with representatives from the relevant European standardisation organisations;

(i) collecting best practice information on risks and incidents;

(j) examining, on an annual basis, the summary reports referred to in the second subparagraph of Article 10(3);

(k) discussing the work undertaken with regard to exercises relating to the security of network and information systems, education programmes and training, including the work done by ENISA;

(l) with ENISA's assistance, exchanging best practice with regard to the identification of operators of essential services by the Member States, including in relation to cross–border dependencies, regarding risks and incidents;

(m) discussing modalities for reporting notifications of incidents as referred to in Articles 14 and 16.

By … [18 months after entry into force of this Directive] and every two years thereafter, the Cooperation Group shall establish a work programme in respect of actions to be undertaken to implement its objectives and tasks, which shall be consistent with the objectives of this Directive.

4. For the purpose of the review referred to in Article 23 and by … [24 months after the date of entry into force of this Directive], and every year and a half thereafter, the Cooperation Group shall prepare a report assessing the experience gained with the strategic cooperation pursued under this Article.

5. The Commission shall adopt implementing acts laying down procedural arrangements necessary for the functioning of the Cooperation Group. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 22(2).

For the purposes of the first subparagraph, the Commission shall submit the first draft implementing act to the committee referred to in Article 22(1) by … [6 months after entry into force of this Directive].

Article 12 CSIRTs network

1. In order to contribute to the development of confidence and trust between the

Member States and to promote swift and effective operational cooperation, a network of the national CSIRTs is hereby established.

2. The CSIRTs network shall be composed of representatives of the Member States' CSIRTs and CERT–EU. The Commission shall participate in the CSIRTs network as an observer. ENISA shall provide the secretariat and shall actively support the cooperation among the CSIRTs.

3. The CSIRTs network shall have the following tasks:

(a) exchanging information on CSIRTs' services, operations and cooperation capabilities;

(b) at the request of a representative of a CSIRT from a Member State potentially affected by an incident, exchanging and discussing non–commercially sensitive information related to that incident and associated risks; however, any

Member State's CSIRT may refuse to contribute to that discussion if there is a risk of prejudice to the investigation of the incident;

(c) exchanging and making available on a voluntary basis non–confidential information concerning individual incidents;

(d) at the request of a representative of a Member State's CSIRT, discussing and, where possible, identifying a coordinated response to an incident that has been identified within the jurisdiction of that same Member State;

(e) providing Member States with support in addressing cross–border incidents on the basis of their voluntary mutual assistance;

(f) discussing, exploring and identifying further forms of operational cooperation, including in relation to:

(i) categories of risks and incidents;

(ii) early warnings;

(iii) mutual assistance;

(iv) principles and modalities for coordination, when Member States respond to cross–border risks and incidents;

(g) informing the Cooperation Group of its activities and of the further forms of operational cooperation discussed pursuant to point (f), and requesting guidance in that regard;

(h) discussing lessons learnt from exercises relating to the security of network and information systems, including from those organised by ENISA;

(i) at the request of an individual CSIRT, discussing the capabilities and preparedness of that CSIRT;

(j) issuing guidelines in order to facilitate the convergence of operational practices with regard to the application of the provisions of this Article concerning operational cooperation.

4. For the purpose of the review referred to in Article 23 and by … [24 months after the date of entry into force of this Directive], and every year and a half thereafter, the CSIRTs network shall produce a report assessing the experience gained with the operational cooperation, including conclusions and recommendations, pursued under this Article. That report shall also be submitted to the Cooperation Group.

5. The CSIRTs network shall lay down its own rules of procedure.

Article 13 International cooperation

The Union may conclude international agreements, in accordance with Article 218 TFEU, with third countries or international organisations, allowing and organising their participation in some activities of the Cooperation Group. Such agreements shall take into account the need to ensure adequate protection of data.

CHAPTER IV SECURITY OF THE NETWORK AND INFORMATION SYSTEMS OF OPERATORS OF ESSENTIAL SERVICES

Article 14. Security requirements and incident notification

1. Member States shall ensure that operators of essential services take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed.

2. Member States shall ensure that operators of essential services take appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of such essential services, with a view to ensuring the continuity of those services.

3. Member States shall ensure that operators of essential services notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact on the continuity of the essential services they provide. Notifications shall include information enabling the competent authority or the CSIRT to determine any cross–border impact of the incident. Notification shall not make the notifying party subject to increased liability.

4. In order to determine the significance of the impact of an incident, the following parameters in particular shall be taken into account:

   (a) the number of users affected by the disruption of the essential service;

   (b) the duration of the incident;

   (c) the geographical spread with regard to the area affected by the incident.

5. On the basis of the information provided in the notification by the operator of essential services, the competent authority or the CSIRT shall inform the other affected Member State(s) if the incident has a significant impact on the continuity of essential services in that Member State. In so doing, the competent authority or the CSIRT shall, in accordance with Union law or national legislation that complies with Union law, preserve the security and commercial interests of the operator of essential services, as well as the confidentiality of the information provided in its notification.

   Where the circumstances allow, the competent authority or the CSIRT shall provide the notifying operator of essential services with relevant information regarding the follow–up of its notification, such as information that could support the effective incident handling.

   At the request of the competent authority or the CSIRT, the single point of contact shall forward notifications as referred to in the first subparagraph to single points of contact of other affected Member States.

6. After consulting the notifying operator of essential services, the competent authority or the CSIRT may inform the public about individual incidents, where public awareness is necessary in order to prevent an incident or to deal with an ongoing incident.

7. Competent authorities acting together within the Cooperation Group may develop and adopt guidelines concerning the circumstances in which operators of

essential services are required to notify incidents, including on the parameters to determine the significance of the impact of an incident as referred to in paragraph 4.

Article 15 Implementation and enforcement

1. Member States shall ensure that the competent authorities have the necessary powers and means to assess the compliance of operators of essential services with their obligations under Article 14 and the effects thereof on the security of network and information systems.

2. Member States shall ensure that the competent authorities have the powers and means to require operators of essential services to provide:

   (a) the information necessary to assess the security of their network and information systems, including documented security policies;

   (b) evidence of the effective implementation of security policies, such as the results of a security audit carried out by the competent authority or a qualified auditor and, in the latter case, to make the results thereof, including the underlying evidence, available to the competent authority.

   When requesting such information or evidence, the competent authority shall state the purpose of the request and specify what information is required.

3. Following the assessment of information or results of security audits referred to in paragraph 2, the competent authority may issue binding instructions to the operators of essential services to remedy the deficiencies identified.

4. The competent authority shall work in close cooperation with data protection authorities when addressing incidents resulting in personal data breaches.

CHAPTER V SECURITY OF THE NETWORK AND INFORMATION SYSTEMS OF DIGITAL SERVICE PROVIDERS

Article 16

Security requirements and incident notification

1. Member States shall ensure that digital service providers identify and take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in the context of offering services referred to in Annex III within the Union. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed, and shall take into account the following elements:

   (a) the security of systems and facilities;

(b) incident handling;

(c) business continuity management;

(d) monitoring, auditing and testing;

(e) compliance with international standards.

2. Member States shall ensure that digital service providers take measures to prevent and minimise the impact of incidents affecting the security of their network and information systems on the services referred to in Annex III that are offered within the Union, with a view to ensuring the continuity of those services.

3. Member States shall ensure that digital service providers notify the competent authority or the CSIRT without undue delay of any incident having a substantial impact on the provision of a service as referred to in Annex III that they offer within the Union. Notifications shall include information to enable the competent authority or the CSIRT to determine the significance of any cross–border impact. Notification shall not make the notifying party subject to increased liability.

4. In order to determine whether the impact of an incident is substantial, the following parameters in particular shall be taken into account:

(a) the number of users affected by the incident, in particular users relying on the service for the provision of their own services;

(b) the duration of the incident;

(c) the geographical spread with regard to the area affected by the incident;

(d) the extent of the disruption of the functioning of the service;

(e) the extent of the impact on economic and societal activities.

The obligation to notify an incident shall only apply where the digital service provider has access to the information needed to assess the impact of an incident against the parameters referred to in the first subparagraph.

5. Where an operator of essential services relies on a third–party digital service provider for the provision of a service which is essential for the maintenance of critical societal and economic activities, any significant impact on the continuity of the essential services due to an incident affecting the digital service provider shall be notified by that operator.

6. Where appropriate, and in particular if the incident referred to in paragraph 3 concerns two or more Member States, the competent authority or the CSIRT shall inform the other affected Member States. In so doing, the competent authorities, CSIRTs and single points of contact shall, in accordance with Union law, or national legislation that complies with Union law, preserve the digital service provider's security and commercial interests as well as the confidentiality of the information provided.

7. After consulting the digital service provider concerned, the competent authority or the CSIRT and, where appropriate, the authorities or the CSIRTs of other Member States concerned may inform the public about individual incidents or require the digital service provider to do so, where public awareness is necessary in order to prevent an incident or to deal with an ongoing incident, or where disclosure of the incident is otherwise in the public interest.

8. The Commission shall adopt implementing acts in order to specify further the elements referred to in paragraph 1 and the parameters listed in paragraph 4 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 22(2) by … [1 year after entry into force of this Directive].

9. The Commission may adopt implementing acts laying down the formats and procedures applicable to notification requirements. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 22(2).

10. Without prejudice to Article 1(6), Member States shall not impose any further security or notification requirements on digital service providers.

11. Chapter V shall not apply to micro– and small enterprises as defined in Commission Recommendation 2003/361/EC[1].

Article 17 Implementation and enforcement

1. Member States shall ensure that the competent authorities take action, if necessary, through *ex post* supervisory measures, when provided with evidence that a digital service provider does not meet the requirements laid down in Article 16. Such evidence may be submitted by a competent authority of another Member State where the service is provided.

---

1 Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium–sized enterprises (OJ L 124, 20.5.2003, p. 36).

2. For the purposes of paragraph 1, the competent authorities shall have the necessary powers and means to require digital service providers to:

   (a) provide the information necessary to assess the security of their network and information systems, including documented security

policies;

(b) remedy any failure to meet the requirements laid down in Article 16.

3. If a digital service provider has its main establishment or a representative in a

Member State, but its network and information systems are located in one or more other Member States, the competent authority of the Member State of the main establishment or of the representative and the competent authorities of those other Member States shall cooperate and assist each other as necessary. Such assistance and cooperation may cover information exchanges between the competent authorities concerned and requests to take the supervisory measures referred to in paragraph 2.

Article 18 Jurisdiction and territoriality

1. For the purposes of this Directive, a digital service provider shall be deemed to be under the jurisdiction of the Member State in which it has its main establishment. A digital service provider shall be deemed to have its main establishment in a Member State when it has its head office in that Member State.

2. A digital service provider that is not established in the Union, but offers services referred to in Annex III within the Union, shall designate a representative in the Union. The representative shall be established in one of those Member States where the services are offered. The digital service provider shall be deemed to be under the jurisdiction of the Member State where the representative is established.

3. The designation of a representative by the digital service provider shall be without prejudice to legal actions which could be initiated against the digital service provider itself.

CHAPTER VI

STANDARDISATION AND VOLUNTARY NOTIFICATION

Article 19 Standardisation

1. In order to promote convergent implementation of Article 14(1) and (2) and Article 16(1) and (2), Member States shall, without imposing or discriminating in favour of the use of a particular type of technology, encourage the use of European or internationally accepted standards and specifications relevant to the security of network and information systems.

2. ENISA, in collaboration with Member States, shall draw up advice and guidelines regarding the technical areas to be considered in relation to paragraph 1 as well as regarding already existing standards, including Member States' national standards, which would allow for those areas to be covered.

Article 20 Voluntary notification

1. Without prejudice to Article 3, entities which have not been identified as operators of essential services and are not digital service providers may notify, on a voluntary basis, incidents having a significant impact on the continuity of the services which they provide.

2. When processing notifications, Member States shall act in accordance with the procedure set out in Article 14. Member States may prioritise the processing of mandatory notifications over voluntary notifications. Voluntary notifications shall only be processed where such processing does not constitute a disproportionate or undue burden on Member States concerned.

Voluntary notification shall not result in the imposition upon the notifying entity of any obligations to which it would not have been subject had it not given that notification.

CHAPTER VII FINAL PROVISIONS

Article 21 Penalties

Member States shall lay down the rules on penalties applicable to infringements of national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive. Member States shall, by … [21 months after the date of entry into force of this Directive], notify the Commission of those rules and of those measures and shall notify it, without delay, of any subsequent amendment affecting them.

Article 22 Committee procedure

1. The Commission shall be assisted by the Network and Information Systems Security Committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

Article 23 Review

1. By … [33 months after the date of entry into force of this Directive], the Commission shall submit a report to the European Parliament and to Council, assessing the consistency of the approach taken by Member States in the identification of the operators of essential services.

2. The Commission shall periodically review the functioning of this Directive and report to the European Parliament and to the Council. For this purpose and with a view to further advancing the strategic and operational cooperation, the Commission shall take into account the reports of the Cooperation Group and the CSIRTs network on the experience gained at a strategic and operational level. In

its review, the Commission shall also assess the lists contained in Annexes II and III, and the consistency in the identification of operators of essential services and services in the sectors referred to in Annex II. The first report shall be submitted by… [57 months after the date of entry into force of this Directive].

Article 24 Transitional measures

1. Without prejudice to Article 25 and with a view to providing Member States with additional possibilities for appropriate cooperation during the period of transposition, the Cooperation Group and the CSIRTs network shall begin to perform the tasks set out in Articles 11(3) and 12(3) respectively by … [6 months after the date of entry into force of this Directive].

2. For the period from … [6 months after the date of entry into force of this Directive] to … [27 months after the date of entry into force of this Directive], and for the purposes of supporting Member States in taking a consistent approach in the process of identification of operators of essential services, the Cooperation Group shall discuss the process, substance and type of national measures allowing for the identification of operators of essential services within a specific sector in accordance with the criteria set out in Articles 5 and 6. The Cooperation Group shall also discuss, at the request of a
   Member State, specific draft national measures of that Member State, allowing for the identification of operators of essential services within a specific sector in accordance with the criteria set out in Articles 5 and 6.

3. By … [6 months after the date of entry into force of this Directive] and for the purposes of this Article, Member States shall ensure appropriate representation in the Cooperation Group and the CSIRTs network.

Article 25 Transposition

1. Member States shall adopt and publish, by … [21 months after the date of entry into force of this Directive], the laws, regulations and administrative provisions necessary to comply with this Directive. They shall immediately inform the Commission thereof.

   They shall apply those measures from … [one day after the date referred to in the first subparagraph].

   When Member States adopt those measures, they shall contain a reference to this Directive or shall be accompanied by such a reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.

2. Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.

Article 26 Entry into force

This Directive shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union.*

Article 27 Addressees

This Directive is addressed to the Member States. Done at Strasbourg,

For the European Parliament *For the Council*

The President *The President*

ANNEX I

Requirements and tasks of computer security incident response teams (CSIRTs)

The requirements and tasks of CSIRTs shall be adequately and clearly defined and supported by national policy and/or regulation. They shall include the following:

(1) Requirements for CSIRTs:

(a) CSIRTs shall ensure a high level of availability of their communications services by avoiding single points of failure, and shall have several means for being contacted and for contacting others at all times. Furthermore, the communication channels shall be clearly specified and well known to the constituency and cooperative partners.

(b) CSIRTs' premises and the supporting information systems shall be located in secure sites.

(c) Business continuity:

(i) CSIRTs shall be equipped with an appropriate system for managing and routing requests, in order to facilitate handovers.

(ii) CSIRTs shall be adequately staffed to ensure availability at all times.

(iii) CSIRTs shall rely on an infrastructure the continuity of which is ensured. To that end, redundant systems and backup working space shall be available.

(d) CSIRTs shall have the possibility to participate, where they wish to

do so, in international cooperation networks.

(2) CSIRTs' tasks:

(a) CSIRTs' tasks shall include at least the following:

(i) monitoring incidents at a national level;

(ii) providing early warning, alerts, announcements and dissemination of information to relevant stakeholders about risks and incidents;

(iii) responding to incidents;

(iv) providing dynamic risk and incident analysis and situational awareness;

(v) participating in the CSIRTs network.

(b) CSIRTs shall establish cooperation relationships with the private sector.

(c) To facilitate cooperation, CSIRTs shall promote the adoption and use of common or standardised practices for:

(i) incident and risk-handling procedures;

(ii) incident, risk and information classification schemes.

ANNEX II

Types of entities for the purposes of point (4) of Article 4

Sector	Subsector	Type of entity
1. Energy	(a) Electricity	— Electricity undertakings as defined in point (35) of Article 2 of Directive 2009/72/EC of the European Parliament and of the Council[1], which carry out the function of 'supply' as defined in point (19) of Article 2 of that Directive

		— Distribution system operators as defined in point (6) of Article 2 of Directive 2009/72/EC
		— Transmission system operators as defined in point (4) of Article 2 of Directive 2009/72/EC
	(b) Oil	— Operators of oil transmission pipelines
		— Operators of oil production, refining and treatment facilities, storage and transmission

1 Directive 2009/72/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC (OJ L 211, 14.8.2009, p. 55).

Sector	Subsector	Type of entity
	(c) Gas	— Supply undertakings as defined in point (8) of Article 2 of Directive 2009/73/EC of the European Parliament and of the Council[1]
		— Distribution system operators as defined in point (6) of Article 2 of Directive 2009/73/EC
		— Transmission system operators as defined in point (4) of Article 2 of Directive 2009/73/EC
		— Storage system operators as defined in point (10) of Article 2 of Directive 2009/73/EC
		— LNG system operators as defined in point (12) of Article 2 of Directive 2009/73/EC
		— Natural gas undertakings as defined in point (1) of Article 2 of Directive 2009/73/EC
		— Operators of natural gas refining and treatment facilities

1 Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC (OJ L 211, 14.8.2009, p. 94).

Sector	Subsector	Type of entity
2. Transport	(a) Air transport	— Air carriers as defined in point (4) of Article 3 of Regulation (EC) No 300/2008 of the European Parliament and of the Council[1]

		— Airport managing bodies as defined in point (2) of Article 2 of Directive 2009/12/EC of the European Parliament and of the Council[2], airports as defined in point (1) of Article 2 of that Directive, including the core airports listed in Section 2 of Annex II to Regulation (EU) No 1315/2013 of the European Parliament and of the Council[3], and entities operating ancillary installations contained within airports
		— Traffic management control operators providing air traffic control (ATC) services as defined in point (1) of Article 2 of Regulation (EC) No 549/2004 of the European Parliament and of the Council[4]

[1] Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (OJ L 97, 9.4.2008, p. 72).

[2] Directive 2009/12/EC of the European Parliament and of the Council of 11 March 2009 on airport charges (OJ L 70, 14.3.2009, p. 11).

[3] Regulation (EU) No 1315/2013 of the European Parliament and of the Council of 11 December 2013 on Union guidelines for the development of the trans–European transport network and repealing Decision No 661/2010/EU (OJ L 348, 20.12.2013, p. 1).

[4] Regulation (EC) No 549/2004 of the European Parliament and of the Council of 10 March 2004 laying down the framework for the creation of the single European sky (the framework Regulation) (OJ L 96, 31.3.2004, p. 1).

Sector	Subsector	Type of entity
	(b) Rail transport	— Infrastructure managers as defined in point (2) of Article 3 of Directive 2012/34/EU of the European Parliament and of the Council[1]
		— Railway undertakings as defined in point (1) of Article 3 of Directive 2012/34/EU, including operators of service facilities as defined in point (12) of Article 3 of Directive 2012/34/EU
	(c) Water transport	— Inland, sea and coastal passenger and freight water transport companies, as defined for maritime transport in Annex I to Regulation (EC) No 725/2004 of the European Parliament and of the Council[2], not including the individual vessels operated by those companies

		— Managing bodies of ports as defined in point (1) of Article 3 of Directive 2005/65/EC of the European Parliament and of the Council[3], including their port facilities as defined in point (11) of Article 2 of Regulation (EC) No 725/2004, and entities operating works and equipment contained within ports

[1] Directive 2012/34/EU of the European Parliament and of the Council of 21 November 2012 establishing a single European railway area (OJ L 343, 14.12.2012, p. 32).

[2] Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security (OJ L 129, 29.4.2004, p. 6).

[3] Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security (OJ L 310, 25.11.2005, p. 28).

Sector	Subsector	Type of entity
		— Operators of vessel traffic services as defined in point (o) of Article 3 of Directive 2002/59/EC of the European Parliament and of the Council[1]
	(d) Road transport	— Road authorities as defined in point (12) of Article 2 of Commission Delegated Regulation (EU) 2015/962[2] responsible for traffic management control
		— Operators of Intelligent Transport Systems as defined in point (1) of Article 4 of Directive 2010/40/EU of the European Parliament and of the Council[3]
3. Banking		Credit institutions as defined in point (1) of Article 4 of Regulation (EU) No 575/2013 of the European Parliament and of the Council[4]

[1] Directive 2002/59/EC of the European Parliament and of the Council of 27 June 2002 establishing a Community vessel traffic monitoring and information system and repealing Council Directive 93/75/EEC (OJ L 208, 5.8.2002, p. 10).

[2] Commission Delegated Regulation (EU) 2015/962 of 18 December 2014 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU–wide real–time traffic information services (OJ L 157, 23.6.2015, p. 21).

[3] Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport (OJ L 207, 6.8.2010, p. 1).

[4] Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013, p. 1).

Sector		Subsector	Type of entity
4.	Financial market infrastructures		— Operators of trading venues as defined in point (24) of Article 4 of Directive 2014/65/EU of the European Parliament and of the Council[1]
			— Central counterparties (CCPs) as defined in point (1) of Article 2 of Regulation (EU) No 648/2012 of the European Parliament and of the Council[2]
5.	Health sector	Health care settings (including hospitals and private clinics)	Healthcare providers as defined in point (g) of Article 3 of Directive 2011/24/EU of the European Parliament and of the Council[3]
6.	Drinking water supply and distribution		Suppliers and distributors of water intended for human consumption as defined in point (1)(a) of Article 2 of Council Directive 98/83/EC[4] but excluding distributors for whom distribution of water for human consumption is only part of their general activity of distributing other commodities and goods which are not considered essential services
7.	Digital Infrastructure		— IXPs
			— DNS service providers
			— TLD name registries

[1] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (OJ L 173, 12.6.2014, p. 349).

[2] Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (OJ L 201, 27.7.2012, p. 1).

[3] Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross–border healthcare (OJ L 88, 4.4.2011, p. 45).

[4] Council Directive 98/83/EC of 3 November 1998 on the quality of water intended for human consumption (OJ L 330, 5.12.1998, p. 32).

ANNEX III

Types of digital services for the purposes of point (5) of Article 4

1. Online marketplace.

2. Online search engine.

3. Cloud computing service.

8. США

8.1. Executive Order -- Improving Critical Infrastructure Cybersecurity, February 12, 2013

(https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity)

The White House
Office of the Press Secretary
For Immediate Release
February 12, 2013
Executive Order -- Improving Critical Infrastructure Cybersecurity
EXECUTIVE ORDER
- - - - - - -
IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:
Section 1. Policy. Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats. It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties. We can achieve these goals through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards.
Sec. 2. Critical Infrastructure. As used in this order, the term critical infrastructure means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.
Sec. 3. Policy Coordination. Policy coordination, guidance, dispute resolution, and periodic in-progress reviews for the functions and programs described and assigned herein shall be provided through the interagency process established in Presidential Policy Directive-1 of February 13, 2009 (Organization of the National Security Council System), or any successor.
Sec. 4. Cybersecurity Information Sharing. (a) It is the policy of the United States Government to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats. Within 120 days of the date of this order, the Attorney General, the Secretary of Homeland Security (the "Secretary"), and the Director of National Intelligence shall each issue instructions consistent with their authorities and with the requirements of section 12(c) of this order to ensure the timely production of unclassified reports of cyber threats to the U.S. homeland that identify a specific targeted entity. The instructions shall address the need to protect intelligence and law enforcement sources, methods, operations, and investigations.

(b) The Secretary and the Attorney General, in coordination with the Director of National Intelligence, shall establish a process that rapidly disseminates the reports produced pursuant to section 4(a) of this order to the targeted entity. Such process shall also, consistent with the need to protect national security information, include the dissemination of classified reports to critical infrastructure entities authorized to receive them. The Secretary and the Attorney General, in coordination with the Director of National Intelligence, shall establish a system for tracking the production, dissemination, and disposition of these reports.

(c) To assist the owners and operators of critical infrastructure in protecting their systems from unauthorized access, exploitation, or harm, the Secretary, consistent with 6 U.S.C. 143 and in collaboration with the Secretary of Defense, shall, within 120 days of the date of this order, establish procedures to expand the Enhanced Cybersecurity Services program to all critical infrastructure sectors. This voluntary information sharing program will provide classified cyber threat and technical information from the Government to eligible critical infrastructure companies or commercial service providers that offer security services to critical infrastructure.

(d) The Secretary, as the Executive Agent for the Classified National Security Information Program created under Executive Order 13549 of August 18, 2010 (Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities), shall expedite the processing of security clearances to appropriate personnel employed by critical infrastructure owners and operators, prioritizing the critical infrastructure identified in section 9 of this order.

(e) In order to maximize the utility of cyber threat information sharing with the private sector, the Secretary shall expand the use of programs that bring private sector subject-matter experts into Federal service on a temporary basis. These subject matter experts should provide advice regarding the content, structure, and types of information most useful to critical infrastructure owners and operators in reducing and mitigating cyber risks.

Sec. 5. Privacy and Civil Liberties Protections. (a) Agencies shall coordinate their activities under this order with their senior agency officials for privacy and civil liberties and ensure that privacy and civil liberties protections are incorporated into such activities. Such protections shall be based upon the Fair Information Practice Principles and other privacy and civil liberties policies, principles, and frameworks as they apply to each agency's activities.

(b) The Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of the Department of Homeland Security (DHS) shall assess the privacy and civil liberties risks of the functions and programs undertaken by DHS as called for in this order and shall recommend to the Secretary ways to minimize or mitigate such risks, in a publicly available report, to be released within 1 year of the date of this order. Senior agency privacy and civil liberties officials for other agencies engaged in activities under this order shall conduct assessments of their agency activities and provide those assessments to DHS for consideration and inclusion in the report. The report shall be reviewed on an annual basis and revised as necessary. The report may contain a classified annex if necessary. Assessments shall include evaluation of activities against the Fair Information Practice Principles and other applicable privacy and civil liberties policies, principles, and frameworks. Agencies shall consider the assessments and recommendations of the report in implementing privacy and civil liberties protections for agency activities.

(c) In producing the report required under subsection (b) of this section, the Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of DHS shall consult with the Privacy and Civil Liberties Oversight Board and coordinate with the Office of Management and Budget (OMB).

(d) Information submitted voluntarily in accordance with 6 U.S.C. 133 by private entities under this order shall be protected from disclosure to the fullest extent permitted by law.

Sec. 6. Consultative Process. The Secretary shall establish a consultative process to coordinate improvements to the cybersecurity of critical infrastructure. As part of the consultative process, the Secretary shall engage and consider the advice, on matters set forth in this order, of the Critical Infrastructure Partnership Advisory Council; Sector Coordinating Councils; critical infrastructure owners and operators; Sector-Specific Agencies; other relevant agencies; independent regulatory agencies; State, local, territorial, and tribal governments; universities; and outside experts.

Sec. 7. Baseline Framework to Reduce Cyber Risk to Critical Infrastructure. (a) The Secretary of Commerce shall direct the Director of the National Institute of Standards and Technology (the "Director") to lead the development of a framework to reduce cyber risks to critical infrastructure (the "Cybersecurity Framework"). The Cybersecurity Framework shall include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks. The Cybersecurity Framework shall incorporate voluntary consensus standards and industry best practices to the fullest extent possible. The Cybersecurity Framework shall be consistent with voluntary international standards when such international standards will advance the objectives of this order, and shall meet the requirements of the National Institute of Standards and Technology Act, as amended (15 U.S.C. 271 et seq.), the National Technology Transfer and Advancement Act of 1995 (Public Law 104-113), and OMB Circular A-119, as revised.

(b) The Cybersecurity Framework shall provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk. The Cybersecurity Framework shall focus on identifying cross-sector security standards and guidelines applicable to critical infrastructure. The Cybersecurity Framework will also identify areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations. To enable technical innovation and account for organizational differences, the Cybersecurity Framework will provide guidance that is technology neutral and that enables critical infrastructure sectors to benefit from a competitive market for products and services that meet the standards, methodologies, procedures, and processes developed to address cyber risks. The Cybersecurity Framework shall include guidance for measuring the performance of an entity in implementing the Cybersecurity Framework.

(c) The Cybersecurity Framework shall include methodologies to identify and mitigate impacts of the Cybersecurity Framework and associated information security measures or controls on business confidentiality, and to protect individual privacy and civil liberties.

(d) In developing the Cybersecurity Framework, the Director shall engage in an open public review and comment process. The Director shall also consult with the Secretary, the National Security Agency, Sector-Specific Agencies and other interested agencies including OMB, owners and operators of critical infrastructure, and other stakeholders through the consultative process established in section 6 of this order. The Secretary, the Director of National Intelligence, and the heads of other relevant agencies shall provide threat and vulnerability information and technical expertise to inform the development of the Cybersecurity Framework. The Secretary shall provide performance goals for the Cybersecurity Framework informed by work under section 9 of this order.

(e) Within 240 days of the date of this order, the Director shall publish a preliminary version of the Cybersecurity Framework (the "preliminary Framework"). Within 1 year of the date of this order, and after coordination with the Secretary to ensure suitability under section 8 of this order, the Director shall publish a final version of the Cybersecurity Framework (the "final Framework").

(f) Consistent with statutory responsibilities, the Director will ensure the Cybersecurity Framework and related guidance is reviewed and updated as necessary, taking into consideration technological changes, changes in cyber risks, operational feedback from owners and operators of critical infrastructure, experience from the implementation of section 8 of this order, and any other relevant factors.

Sec. 8. Voluntary Critical Infrastructure Cybersecurity Program. (a) The Secretary, in coordination with Sector-Specific Agencies, shall establish a voluntary program to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and any other interested entities (the "Program").

(b) Sector-Specific Agencies, in consultation with the Secretary and other interested agencies, shall coordinate with the Sector Coordinating Councils to review the Cybersecurity Framework and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments.

(c) Sector-Specific Agencies shall report annually to the President, through the Secretary, on the extent to which owners and operators notified under section 9 of this order are participating in the Program.

(d) The Secretary shall coordinate establishment of a set of incentives designed to promote participation in the Program. Within 120 days of the date of this order, the Secretary and the Secretaries of the Treasury and Commerce each shall make recommendations separately to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs, that shall include analysis of the benefits and relative effectiveness of such incentives, and whether the incentives would require legislation or can be provided under existing law and authorities to participants in the Program.

(e) Within 120 days of the date of this order, the Secretary of Defense and the Administrator of General Services, in consultation with the Secretary and the Federal Acquisition Regulatory Council, shall make recommendations to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs, on the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration. The report shall address what steps can be taken to harmonize and make consistent existing procurement requirements related to cybersecurity.

Sec. 9. Identification of Critical Infrastructure at Greatest Risk. (a) Within 150 days of the date of this order, the Secretary shall use a risk-based approach to identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security. In identifying critical infrastructure for this purpose, the Secretary shall use the consultative process established in section 6 of this order and draw upon the expertise of Sector-Specific Agencies. The Secretary shall apply consistent, objective criteria in identifying such critical infrastructure. The Secretary shall not identify any commercial information technology products or consumer information technology services under this section. The Secretary shall review and update the list of identified critical infrastructure under this section on an annual basis, and provide such list to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs.

(b) Heads of Sector-Specific Agencies and other relevant agencies shall provide the Secretary with information necessary to carry out the responsibilities under this section. The Secretary shall develop a process for other relevant stakeholders to submit information to assist in making the identifications required in subsection (a) of this section.

(c) The Secretary, in coordination with Sector-Specific Agencies, shall confidentially notify owners and operators of critical infrastructure identified under subsection (a) of this section that they have been so identified, and ensure identified owners and operators are provided the basis for the determination. The Secretary shall establish a process through which owners and operators of critical infrastructure may submit relevant information and request reconsideration of identifications under subsection (a) of this section.

Sec. 10. Adoption of Framework. (a) Agencies with responsibility for regulating the security of critical infrastructure shall engage in a consultative process with DHS, OMB, and the National Security Staff to review the preliminary Cybersecurity Framework and determine if current cybersecurity regulatory requirements are sufficient given current and projected risks. In making such determination, these agencies shall consider the identification of critical infrastructure required under section 9 of this order. Within 90 days of the publication of the preliminary Framework, these agencies shall submit a report to the President, through the Assistant to the President for Homeland Security and Counterterrorism, the Director of OMB, and the Assistant to the President for Economic Affairs, that states whether or not the agency has clear authority to establish requirements based upon the Cybersecurity Framework to sufficiently address current and projected cyber risks to critical infrastructure, the existing authorities identified, and any additional authority required.

(b) If current regulatory requirements are deemed to be insufficient, within 90 days of publication of the final Framework, agencies identified in subsection (a) of this section shall propose prioritized, risk-based, efficient, and coordinated actions, consistent with Executive Order 12866 of September 30, 1993 (Regulatory Planning and Review), Executive Order 13563 of January 18, 2011 (Improving Regulation and Regulatory Review), and Executive Order 13609 of May 1, 2012 (Promoting International Regulatory Cooperation), to mitigate cyber risk.

(c) Within 2 years after publication of the final Framework, consistent with Executive Order 13563 and Executive Order 13610 of May 10, 2012 (Identifying and Reducing Regulatory Burdens), agencies identified in subsection (a) of this section shall, in consultation with owners and operators of critical infrastructure, report to OMB on any critical infrastructure subject to ineffective, conflicting, or excessively burdensome cybersecurity requirements. This report shall describe efforts made by agencies, and make recommendations for further actions, to minimize or eliminate such requirements.

(d) The Secretary shall coordinate the provision of technical assistance to agencies identified in subsection (a) of this section on the development of their cybersecurity workforce and programs.

(e) Independent regulatory agencies with responsibility for regulating the security of critical infrastructure are encouraged to engage in a consultative process with the Secretary, relevant Sector-Specific Agencies, and other affected parties to consider prioritized actions to mitigate cyber risks for critical infrastructure consistent with their authorities.

Sec. 11. Definitions. (a) "Agency" means any authority of the United States that is an "agency" under 44 U.S.C. 3502(1), other than those considered to be independent regulatory agencies, as defined in 44 U.S.C. 3502(5).

(b) "Critical Infrastructure Partnership Advisory Council" means the council established by DHS under 6 U.S.C. 451 to facilitate effective interaction and coordination of critical infrastructure protection activities among the Federal Government; the private sector; and State, local, territorial, and tribal governments.

(c) "Fair Information Practice Principles" means the eight principles set forth in Appendix A of the National Strategy for Trusted Identities in Cyberspace.

(d) "Independent regulatory agency" has the meaning given the term in 44 U.S.C. 3502(5).

(e) "Sector Coordinating Council" means a private sector coordinating council composed of representatives of owners and operators within a particular sector of critical infrastructure established by the National Infrastructure Protection Plan or any successor.
(f) "Sector-Specific Agency" has the meaning given the term in Presidential Policy Directive-21 of February 12, 2013 (Critical Infrastructure Security and Resilience), or any successor.
Sec. 12. General Provisions. (a) This order shall be implemented consistent with applicable law and subject to the availability of appropriations. Nothing in this order shall be construed to provide an agency with authority for regulating the security of critical infrastructure in addition to or to a greater extent than the authority the agency has under existing law. Nothing in this order shall be construed to alter or limit any authority or responsibility of an agency under existing law.
(b) Nothing in this order shall be construed to impair or otherwise affect the functions of the Director of OMB relating to budgetary, administrative, or legislative proposals.
(c) All actions taken pursuant to this order shall be consistent with requirements and authorities to protect intelligence and law enforcement sources and methods. Nothing in this order shall be interpreted to supersede measures established under authority of law to protect the security and integrity of specific activities and associations that are in direct support of intelligence and law enforcement operations.
(d) This order shall be implemented consistent with U.S. international obligations.
(e) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

BARACK OBAMA

8.2. Presidential Policy Directive -- Critical Infrastructure Security and Resilience, February 12, 2013

(https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil)

Presidential Policy Directive -- Critical Infrastructure Security and Resilience
PRESIDENTIAL POLICY DIRECTIVE/PPD-21

SUBJECT: Critical Infrastructure Security and Resilience

The Presidential Policy Directive (PPD) on Critical Infrastructure Security and Resilience advances a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure.

Introduction

The Nation's critical infrastructure provides the essential services that underpin American society. Proactive and coordinated efforts are necessary to strengthen and maintain secure, functioning, and resilient critical infrastructure – including assets, networks, and systems – that are vital to public confidence and the Nation's safety, prosperity, and well-being.
The Nation's critical infrastructure is diverse and complex. It includes distributed networks, varied organizational structures and operating models (including multinational ownership), interdependent functions and systems in both the physical space and cyberspace, and governance constructs that involve multi-level authorities, responsibilities, and regulations. Critical infrastructure owners and operators are uniquely positioned to manage risks to their individual operations and assets, and to determine effective strategies to make them more secure and resilient.
Critical infrastructure must be secure and able to withstand and rapidly recover from all hazards. Achieving this will require integration with the national preparedness system across prevention, protection, mitigation, response, and recovery.
This directive establishes national policy on critical infrastructure security and resilience. This endeavor is a shared responsibility among the Federal, state, local, tribal, and territorial (SLTT) entities, and public and private owners and operators of critical infrastructure (herein referred to as "critical infrastructure owners and operators"). This directive also refines and clarifies the critical infrastructure-related functions, roles, and responsibilities across the Federal Government, as well as enhances overall coordination and collaboration. The Federal Government also has a responsibility to strengthen the security and resilience of its own critical infrastructure, for the continuity of national essential functions, and to organize itself to partner effectively with and add value to the security and resilience efforts of critical infrastructure owners and operators.

Policy

It is the policy of the United States to strengthen the security and resilience of its critical infrastructure against both physical and cyber threats. The Federal Government shall work with critical infrastructure owners and operators and SLTT entities to take proactive steps to manage risk and strengthen the security and resilience of the Nation's critical infrastructure, considering all hazards that could have a debilitating impact on national security, economic stability, public health and safety, or any combination thereof. These efforts shall seek to

reduce vulnerabilities, minimize consequences, identify and disrupt threats, and hasten response and recovery efforts related to critical infrastructure.
The Federal Government shall also engage with international partners to strengthen the security and resilience of domestic critical infrastructure and critical infrastructure located outside of the United States on which the Nation depends.
U.S. efforts shall address the security and resilience of critical infrastructure in an integrated, holistic manner to reflect this infrastructure's interconnectedness and interdependency. This directive also identifies energy and communications systems as uniquely critical due to the enabling functions they provide across all critical infrastructure sectors.
Three strategic imperatives shall drive the Federal approach to strengthen critical infrastructure security and resilience:
1) Refine and clarify functional relationships across the Federal Government to advance the national unity of effort to strengthen critical infrastructure security and resilience;
2) Enable effective information exchange by identifying baseline data and systems requirements for the Federal Government; and
3) Implement an integration and analysis function to inform planning and operations decisions regarding critical infrastructure.
All Federal department and agency heads are responsible for the identification, prioritization, assessment, remediation, and security of their respective internal critical infrastructure that supports primary mission essential functions. Such infrastructure shall be addressed in the plans and execution of the requirements in the National Continuity Policy.
Federal departments and agencies shall implement this directive in a manner consistent with applicable law, Presidential directives, and Federal regulations, including those protecting privacy, civil rights, and civil liberties. In addition, Federal departments and agencies shall protect all information associated with carrying out this directive consistent with applicable legal authorities and policies.

Roles and Responsibilities

Effective implementation of this directive requires a national unity of effort pursuant to strategic guidance from the Secretary of Homeland Security. That national effort must include expertise and day-to-day engagement from the Sector-Specific Agencies (SSAs) as well as the specialized or support capabilities from other Federal departments and agencies, and strong collaboration with critical infrastructure owners and operators and SLTT entities. Although the roles and responsibilities identified in this directive are directed at Federal departments and agencies, effective partnerships with critical infrastructure owners and operators and SLTT entities are imperative to strengthen the security and resilience of the Nation's critical infrastructure.

Secretary of Homeland Security

The Secretary of Homeland Security shall provide strategic guidance, promote a national unity of effort, and coordinate the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure. In carrying out the responsibilities assigned in the Homeland Security Act of 2002, as amended, the Secretary of Homeland Security evaluates national capabilities, opportunities, and challenges in protecting critical infrastructure; analyzes threats to, vulnerabilities of, and potential consequences from all hazards on critical infrastructure; identifies security and resilience functions that are necessary for effective public-private engagement with all critical infrastructure sectors; develops a national plan and metrics, in coordination with SSAs and other critical infrastructure partners; integrates and

coordinates Federal cross-sector security and resilience activities; identifies and analyzes key interdependencies among critical infrastructure sectors; and reports on the effectiveness of national efforts to strengthen the Nation's security and resilience posture for critical infrastructure.

Additional roles and responsibilities for the Secretary of Homeland Security include:

1) Identify and prioritize critical infrastructure, considering physical and cyber threats, vulnerabilities, and consequences, in coordination with SSAs and other Federal departments and agencies;

2) Maintain national critical infrastructure centers that shall provide a situational awareness capability that includes integrated, actionable information about emerging trends, imminent threats, and the status of incidents that may impact critical infrastructure;

3) In coordination with SSAs and other Federal departments and agencies, provide analysis, expertise, and other technical assistance to critical infrastructure owners and operators and facilitate access to and exchange of information and intelligence necessary to strengthen the security and resilience of critical infrastructure;

4) Conduct comprehensive assessments of the vulnerabilities of the Nation's critical infrastructure in coordination with the SSAs and in collaboration with SLTT entities and critical infrastructure owners and operators;

5) Coordinate Federal Government responses to significant cyber or physical incidents affecting critical infrastructure consistent with statutory authorities;

6) Support the Attorney General and law enforcement agencies with their responsibilities to investigate and prosecute threats to and attacks against critical infrastructure;

7) Coordinate with and utilize the expertise of SSAs and other appropriate Federal departments and agencies to map geospatially, image, analyze, and sort critical infrastructure by employing commercial satellite and airborne systems, as well as existing capabilities within other departments and agencies; and

8) Report annually on the status of national critical infrastructure efforts as required by statute.

Sector-Specific Agencies

Each critical infrastructure sector has unique characteristics, operating models, and risk profiles that benefit from an identified Sector-Specific Agency that has institutional knowledge and specialized expertise about the sector. Recognizing existing statutory or regulatory authorities of specific Federal departments and agencies, and leveraging existing sector familiarity and relationships, SSAs shall carry out the following roles and responsibilities for their respective sectors:

1) As part of the broader national effort to strengthen the security and resilience of critical infrastructure, coordinate with the Department of Homeland Security (DHS) and other relevant Federal departments and agencies and collaborate with critical infrastructure owners and operators, where appropriate with independent regulatory agencies, and with SLTT entities, as appropriate, to implement this directive;

2) Serve as a day-to-day Federal interface for the dynamic prioritization and coordination of sector-specific activities;

3) Carry out incident management responsibilities consistent with statutory authority and other appropriate policies, directives, or regulations;

4) Provide, support, or facilitate technical assistance and consultations for that sector to identify vulnerabilities and help mitigate incidents, as appropriate; and

5) Support the Secretary of Homeland Security's statutorily required reporting requirements by providing on an annual basis sector-specific critical infrastructure information.

Additional Federal Responsibilities

The following departments and agencies have specialized or support functions related to critical infrastructure security and resilience that shall be carried out by, or along with, other Federal departments and agencies and independent regulatory agencies, as appropriate.

1) The Department of State, in coordination with DHS, SSAs, and other Federal departments and agencies, shall engage foreign governments and international organizations to strengthen the security and resilience of critical infrastructure located outside the United States and to facilitate the overall exchange of best practices and lessons learned for promoting the security and resilience of critical infrastructure on which the Nation depends.

2) The Department of Justice (DOJ), including the Federal Bureau of Investigation (FBI), shall lead counterterrorism and counterintelligence investigations and related law enforcement activities across the critical infrastructure sectors. DOJ shall investigate, disrupt, prosecute, and otherwise reduce foreign intelligence, terrorist, and other threats to, and actual or attempted attacks on, or sabotage of, the Nation's critical infrastructure. The FBI also conducts domestic collection, analysis, and dissemination of cyber threat information, and shall be responsible for the operation of the National Cyber Investigative Joint Task Force (NCIJTF). The NCIJTF serves as a multi-agency national focal point for coordinating, integrating, and sharing pertinent information related to cyber threat investigations, with representation from DHS, the Intelligence Community (IC), the Department of Defense (DOD), and other agencies as appropriate. The Attorney General and the Secretary of Homeland Security shall collaborate to carry out their respective critical infrastructure missions.

3) The Department of the Interior, in collaboration with the SSA for the Government Facilities Sector, shall identify, prioritize, and coordinate the security and resilience efforts for national monuments and icons and incorporate measures to reduce risk to these critical assets, while also promoting their use and enjoyment.

4) The Department of Commerce (DOC), in collaboration with DHS and other relevant Federal departments and agencies, shall engage private sector, research, academic, and government organizations to improve security for technology and tools related to cyber-based systems, and promote the development of other efforts related to critical infrastructure to enable the timely availability of industrial products, materials, and services to meet homeland security requirements.

5) The IC, led by the Director of National Intelligence (DNI), shall use applicable authorities and coordination mechanisms to provide, as appropriate, intelligence assessments regarding threats to critical infrastructure and coordinate on intelligence and other sensitive or proprietary information related to critical infrastructure. In addition, information security policies, directives, standards, and guidelines for safeguarding national security systems shall be overseen as directed by the President, applicable law, and in accordance with that direction, carried out under the authority of the heads of agencies that operate or exercise authority over such national security systems.

6) The General Services Administration, in consultation with DOD, DHS, and other departments and agencies as appropriate, shall provide or support government-wide contracts for critical infrastructure systems and ensure that such contracts include audit rights for the security and resilience of critical infrastructure.

7) The Nuclear Regulatory Commission (NRC) is to oversee its licensees' protection of commercial nuclear power reactors and non-power nuclear reactors used for research, testing, and training; nuclear materials in medical, industrial, and academic settings, and facilities that fabricate nuclear fuel; and the transportation, storage, and disposal of nuclear materials and

waste. The NRC is to collaborate, to the extent possible, with DHS, DOJ, the Department of Energy, the Environmental Protection Agency, and other Federal departments and agencies, as appropriate, on strengthening critical infrastructure security and resilience.
8) The Federal Communications Commission, to the extent permitted by law, is to exercise its authority and expertise to partner with DHS and the Department of State, as well as other Federal departments and agencies and SSAs as appropriate, on: (1) identifying and prioritizing communications infrastructure; (2) identifying communications sector vulnerabilities and working with industry and other stakeholders to address those vulnerabilities; and (3) working with stakeholders, including industry, and engaging foreign governments and international organizations to increase the security and resilience of critical infrastructure within the communications sector and facilitating the development and implementation of best practices promoting the security and resilience of critical communications infrastructure on which the Nation depends.
9) Federal departments and agencies shall provide timely information to the Secretary of Homeland Security and the national critical infrastructure centers necessary to support cross-sector analysis and inform the situational awareness capability for critical infrastructure.

Three Strategic Imperatives

1) Refine and Clarify Functional Relationships across the Federal Government to Advance the National Unity of Effort to Strengthen Critical Infrastructure Security and Resilience
An effective national effort to strengthen critical infrastructure security and resilience must be guided by a national plan that identifies roles and responsibilities and is informed by the expertise, experience, capabilities, and responsibilities of the SSAs, other Federal departments and agencies with critical infrastructure roles, SLTT entities, and critical infrastructure owners and operators.
During the past decade, new programs and initiatives have been established to address specific infrastructure issues, and priorities have shifted and expanded. As a result, Federal functions related to critical infrastructure security and resilience shall be clarified and refined to establish baseline capabilities that will reflect this evolution of knowledge, to define relevant Federal program functions, and to facilitate collaboration and information exchange between and among the Federal Government, critical infrastructure owners and operators, and SLTT entities.
As part of this refined structure, there shall be two national critical infrastructure centers operated by DHS – one for physical infrastructure and another for cyber infrastructure. They shall function in an integrated manner and serve as focal points for critical infrastructure partners to obtain situational awareness and integrated, actionable information to protect the physical and cyber aspects of critical infrastructure. Just as the physical and cyber elements of critical infrastructure are inextricably linked, so are the vulnerabilities. Accordingly, an integration and analysis function (further developed in Strategic Imperative 3) shall be implemented between these two national centers.
The success of these national centers, including the integration and analysis function, is dependent on the quality and timeliness of the information and intelligence they receive from the SSAs and other Federal departments and agencies, as well as from critical infrastructure owners and operators and SLTT entities.
These national centers shall not impede the ability of the heads of Federal departments and agencies to carry out or perform their responsibilities for national defense, criminal, counterintelligence, counterterrorism, or investigative activities.

2) Enable Efficient Information Exchange by Identifying Baseline Data and Systems Requirements for the Federal Government

A secure, functioning, and resilient critical infrastructure requires the efficient exchange of information, including intelligence, between all levels of governments and critical infrastructure owners and operators. This must facilitate the timely exchange of threat and vulnerability information as well as information that allows for the development of a situational awareness capability during incidents. The goal is to enable efficient information exchange through the identification of requirements for data and information formats and accessibility, system interoperability, and redundant systems and alternate capabilities should there be a disruption in the primary systems.
Greater information sharing within the government and with the private sector can and must be done while respecting privacy and civil liberties. Federal departments and agencies shall ensure that all existing privacy principles, policies, and procedures are implemented consistent with applicable law and policy and shall include senior agency officials for privacy in their efforts to govern and oversee information sharing properly.

3) Implement an Integration and Analysis Function to Inform Planning and Operational Decisions Regarding Critical Infrastructure
The third strategic imperative builds on the first two and calls for the implementation of an integration and analysis function for critical infrastructure that includes operational and strategic analysis on incidents, threats, and emerging risks. It shall reside at the intersection of the two national centers as identified in Strategic Imperative 1, and it shall include the capability to collate, assess, and integrate vulnerability and consequence information with threat streams and hazard information to:
a. Aid in prioritizing assets and managing risks to critical infrastructure;
b. Anticipate interdependencies and cascading impacts;
c. Recommend security and resilience measures for critical infrastructure prior to, during, and after an event or incident; and
d. Support incident management and restoration efforts related to critical infrastructure.

This function shall not replicate the analysis function of the IC or the National Counterterrorism Center, nor shall it involve intelligence collection activities. The IC, DOD, DOJ, DHS, and other Federal departments and agencies with relevant intelligence or information shall, however, inform this integration and analysis capability regarding the Nation's critical infrastructure by providing relevant, timely, and appropriate information to the national centers. This function shall also use information and intelligence provided by other critical infrastructure partners, including SLTT and nongovernmental analytic entities.
Finally, this integration and analysis function shall support DHS's ability to maintain and share, as a common Federal service, a near real-time situational awareness capability for critical infrastructure that includes actionable information about imminent threats, significant trends, and awareness of incidents that may affect critical infrastructure.

Innovation and Research and Development

The Secretary of Homeland Security, in coordination with the Office of Science and Technology Policy (OSTP), the SSAs, DOC, and other Federal departments and agencies, shall provide input to align those Federal and Federally-funded research and development (R&D) activities that seek to strengthen the security and resilience of the Nation's critical infrastructure, including:

1) Promoting R&D to enable the secure and resilient design and construction of critical infrastructure and more secure accompanying cyber technology;
2) Enhancing modeling capabilities to determine potential impacts on critical infrastructure of an incident or threat scenario, as well as cascading effects on other sectors;
3) Facilitating initiatives to incentivize cybersecurity investments and the adoption of critical infrastructure design features that strengthen all-hazards security and resilience; and
4) Prioritizing efforts to support the strategic guidance issued by the Secretary of Homeland Security.

Implementation of the Directive

The Secretary of Homeland Security shall take the following actions as part of the implementation of this directive.

1) Critical Infrastructure Security and Resilience Functional Relationships. Within 120 days of the date of this directive, the Secretary of Homeland Security shall develop a description of the functional relationships within DHS and across the Federal Government related to critical infrastructure security and resilience. It should include the roles and functions of the two national critical infrastructure centers and a discussion of the analysis and integration function. When complete, it should serve as a roadmap for critical infrastructure owners and operators and SLTT entities to navigate the Federal Government's functions and primary points of contact assigned to those functions for critical infrastructure security and resilience against both physical and cyber threats. The Secretary shall coordinate this effort with the SSAs and other relevant Federal departments and agencies. The Secretary shall provide the description to the President through the Assistant to the President for Homeland Security and Counterterrorism.

2) Evaluation of the Existing Public-Private Partnership Model. Within 150 days of the date of this directive, the Secretary of Homeland Security, in coordination with the SSAs, other relevant Federal departments and agencies, SLTT entities, and critical infrastructure owners and operators, shall conduct an analysis of the existing public-private partnership model and recommend options for improving the effectiveness of the partnership in both the physical and cyber space. The evaluation shall consider options to streamline processes for collaboration and exchange of information and to minimize duplication of effort. Furthermore, the analysis shall consider how the model can be flexible and adaptable to meet the unique needs of individual sectors while providing a focused, disciplined, and effective approach for the Federal Government to coordinate with the critical infrastructure owners and operators and with SLTT governments. The evaluation shall result in recommendations to enhance partnerships to be approved for implementation through the processes established in the Organization of the National Security Council System directive.

3) Identification of Baseline Data and Systems Requirements for the Federal Government to Enable Efficient Information Exchange. Within 180 days of the date of this directive, the Secretary of Homeland Security, in coordination with the SSAs and other Federal departments and agencies, shall convene a team of experts to identify baseline data and systems requirements to enable the efficient exchange of information and intelligence relevant to strengthening the security and resilience of critical infrastructure. The experts should include representatives from those entities that routinely possess information important to critical infrastructure security and resilience; those that determine and manage information technology systems used to exchange information; and those responsible for the

security of information being exchanged. Interoperability with critical infrastructure partners; identification of key data and the information requirements of key Federal, SLTT, and private sector entities; availability, accessibility, and formats of data; the ability to exchange various classifications of information; and the security of those systems to be used; and appropriate protections for individual privacy and civil liberties should be included in the analysis. The analysis should result in baseline requirements for sharing of data and interoperability of systems to enable the timely exchange of data and information to secure critical infrastructure and make it more resilient. The Secretary shall provide that analysis to the President through the Assistant to the President for Homeland Security and Counterterrorism.

4) Development of a Situational Awareness Capability for Critical Infrastructure. Within 240 days of the date of this directive, the Secretary of Homeland Security shall demonstrate a near real-time situational awareness capability for critical infrastructure that includes threat streams and all-hazards information as well as vulnerabilities; provides the status of critical infrastructure and potential cascading effects; supports decision making; and disseminates critical information that may be needed to save or sustain lives, mitigate damage, or reduce further degradation of a critical infrastructure capability throughout an incident. This capability should be available for and cover physical and cyber elements of critical infrastructure, and enable an integration of information as necessitated by the incident.

5) Update to National Infrastructure Protection Plan. Within 240 days of the date of this directive, the Secretary of Homeland Security shall provide to the President, through the Assistant to the President for Homeland Security and Counterterrorism, a successor to the National Infrastructure Protection Plan to address the implementation of this directive, the requirements of Title II of the Homeland Security Act of 2002 as amended, and alignment with the National Preparedness Goal and System required by PPD-8. The plan shall include the identification of a risk management framework to be used to strengthen the security and resilience of critical infrastructure; the methods to be used to prioritize critical infrastructure; the protocols to be used to synchronize communication and actions within the Federal Government; and a metrics and analysis process to be used to measure the Nation's ability to manage and reduce risks to critical infrastructure. The updated plan shall also reflect the identified functional relationships within DHS and across the Federal Government and the updates to the public-private partnership model. Finally, the plan should consider sector dependencies on energy and communications systems, and identify pre-event and mitigation measures or alternate capabilities during disruptions to those systems. The Secretary shall coordinate this effort with the SSAs, other relevant Federal departments and agencies, SLTT entities, and critical infrastructure owners and operators.

6) National Critical Infrastructure Security and Resilience R&D Plan. Within 2 years of the date of this directive, the Secretary of Homeland Security, in coordination with the OSTP, the SSAs, DOC, and other Federal departments and agencies, shall provide to the President, through the Assistant to the President for Homeland Security and Counterterrorism, a National Critical Infrastructure Security and Resilience R&D Plan that takes into account the evolving threat landscape, annual metrics, and other relevant information to identify priorities and guide R&D requirements and investments. The plan should be issued every 4 years after its initial delivery, with interim updates as needed.

Policy coordination, dispute resolution, and periodic in-progress reviews for the implementation of this directive shall be carried out consistent with PPD-1, including the use of Interagency Policy Committees coordinated by the National Security Staff.

Nothing in this directive alters, supersedes, or impedes the authorities of Federal departments and agencies, including independent regulatory agencies, to carry out their functions and

duties consistent with applicable legal authorities and other Presidential guidance and directives, including, but not limited to, the designation of critical infrastructure under such authorities.
This directive revokes Homeland Security Presidential Directive/HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection, issued December 17, 2003. Plans developed pursuant to HSPD-7 shall remain in effect until specifically revoked or superseded.

Designated Critical Infrastructure Sectors and Sector-Specific Agencies
This directive identifies 16 critical infrastructure sectors and designates associated Federal SSAs. In some cases co-SSAs are designated where those departments share the roles and responsibilities of the SSA. The Secretary of Homeland Security shall periodically evaluate the need for and approve changes to critical infrastructure sectors and shall consult with the Assistant to the President for Homeland Security and Counterterrorism before changing a critical infrastructure sector or a designated SSA for that sector. The sectors and SSAs are as follows:
Chemical:
Sector-Specific Agency: Department of Homeland Security
Commercial Facilities:
Sector-Specific Agency: Department of Homeland Security
Communications:
Sector-Specific Agency: Department of Homeland Security
Critical Manufacturing: Sector-Specific Agency: Department of Homeland Security
Dams:
Sector-Specific Agency: Department of Homeland Security
Defense Industrial Base:
Sector-Specific Agency: Department of Defense
Emergency Services:
Sector-Specific Agency: Department of Homeland Security
Energy:
Sector-Specific Agency: Department of Energy
Financial Services:
Sector-Specific Agency: Department of the Treasury
Food and Agriculture:
Co-Sector-Specific Agencies: U.S. Department of Agriculture and Department of Health and Human Services
Government Facilities:
Co-Sector-Specific Agencies: Department of Homeland Security and General Services Administration
Healthcare and Public Health:
Sector-Specific Agency: Department of Health and Human Services
Information Technology:
Sector-Specific Agency: Department of Homeland Security
Nuclear Reactors, Materials, and Waste:
Sector-Specific Agency: Department of Homeland Security
Transportation Systems:
Co-Sector-Specific Agencies: Department of Homeland Security and Department of Transportation
Water and Wastewater Systems:
Sector-Specific Agency: Environmental Protection Agency

Definitions

For purposes of this directive:
The term "all hazards" means a threat or an incident, natural or manmade, that warrants action to protect life, property, the environment, and public health or safety, and to minimize disruptions of government, social, or economic activities. It includes natural disasters, cyber incidents, industrial accidents, pandemics, acts of terrorism, sabotage, and destructive criminal activity targeting critical infrastructure.
The term "collaboration" means the process of working together to achieve shared goals.
The terms "coordinate" and "in coordination with" mean a consensus decision-making process in which the named coordinating department or agency is responsible for working with the affected departments and agencies to achieve consensus and a consistent course of action.
The term "critical infrastructure" has the meaning provided in section 1016(e) of the USA Patriot Act of 2001 (42 U.S.C. 5195c(e)), namely systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.
The term "Federal departments and agencies" means any authority of the United States that is an "agency" under 44 U.S.C. 3502(1), other than those considered to be independent regulatory agencies, as defined in 44 U.S.C. 3502(5).
The term "national essential functions" means that subset of Government functions that are necessary to lead and sustain the Nation during a catastrophic emergency.
The term "primary mission essential functions" means those Government functions that must be performed in order to support or implement the performance of the national essential functions before, during, and in the aftermath of an emergency.
The term "national security systems" has the meaning given to it in the Federal Information Security Management Act of 2002 (44 U.S.C. 3542(b)).
The term "resilience" means the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.
The term "Sector-Specific Agency" (SSA) means the Federal department or agency designated under this directive to be responsible for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment.
The terms "secure" and "security" refer to reducing the risk to critical infrastructure by physical means or defense cyber measures to intrusions, attacks, or the effects of natural or manmade disasters.