ALERT MEMORANDUM

Italian National Cybersecurity Perimeter: Some Considerations Following Completion of The Regulatory Framework

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors.

ROME
Piazza di Spagna 15
00187 Rome, Italy
T: +39 06 69 52 21

Andrea Mantovani
+39 06 6952 2804
amantovani@cgsh.com

Federica Mammì Borruto
+39 06 6952 2826
fmammiborruto@cgsh.com

MILAN
Via San Paolo 57
20121 Milan, Italy
T: +39 02 72 60 81

Lorenzo Freddi
+39 02 7260 8630
lfreddi@cgsh.com

April 17, 2023

On January 10, 2023, the Resolution of the National Cybersecurity Agency's ("**ACN**") of January 3, 2023 (the "**Resolution**"), which includes the taxonomy of incidents affecting networks, information systems, and information services other than ICT Assets (as defined below) to be notified by entities included in the National Cybersecurity Perimeter (the "**PSNC**")[1], was published in the Italian Official Journal.

Therefore, the regulatory framework on the PSNC is now complete, although the list of accredited testing laboratories ("**LAP**") that can perform the tests prescribed by the National Assessment and Certification Center ("**CVCN**") remains to be established.

The Resolution became effective on January 25, 2023 and provides a useful opportunity to reflect more broadly on the regulatory framework applicable to PSNC. Indeed, the regulatory framework applies not only to the entities included in the PSNC, but also to third-party providers of assets and services that operate on the systems owned by the entities included in the PSNC. In particular, such third-party providers, in addition to being the direct recipients of specific obligations under the PSNC framework, must also ensure that their offerings comply with the obligations to which their customers included in the PSNC are subject.

Therefore, it is essential that all the parties involved consider implementing a corporate cybersecurity organizational model that takes into account the aforementioned regulatory framework, defines the processes potentially affected and formalizes effective technical and organizational measures to mitigate any risks.

[1] Article 1(3-*bis*) of Law Decree No. 105/2019.

I. The PSNC regulatory framework

The regulatory framework of the PSNC[2] is addressed to national public and private entities identified by an administrative act of the Prime Minister (not subject to publication). Such entities perform an essential function or service or have a strategic role for the national interests and, in particular, operate networks, information systems and IT services, the malfunction or interruption (even partial) or improper use of which may jeopardize national security (the "**ICT Assets**"). The ACN[3] will inform the aforementioned entities of their inclusion in the PSNC, indicating the essential function or service.

Obligations of the entities included in the PSNC

The obligations of the entities included in the PSNC cover, among other things, the following:

- preparation and submission to ACN of a list of ICT Assets;
- adoption of security measures for ICT Assets;
- notification to CSIRT (Computer Security Incident Response Team) Italia and management of security incidents affecting ICT Assets or assets included in Annex A of the Resolution;
- notification to the CVCN and compliance with appropriate technology review procedures for procurements of relevant technology assets.

Submission of the list of ICT Assets

Entities included in the PSNC must submit a list of ICT Assets within six months of receiving notification of inclusion in the PSNC.[4]

The list must be updated and submitted to the ACN at least once a year. In the event of significant changes, the list of ICT Assets and the template describing the security measures implemented by the entities included in the PSNC must be updated and submitted to the ACN.

Security Measures

The security measures to be adopted by the entities included in the PSNC are specified in Annex B of DPCM 81/2021 and are divided into two categories (A and B) – depending on their complexity (with category B security measures being the most burdensome, including localization requirements) – with different implementation times.

The security measures for ICT Assets relate to:

- organizational structure responsible for security management;
- security policies and risk management;
- incident mitigation, management and prevention, including intervention on equipment or products found to be seriously insecure;
- physical, logical and data protection;
- network and information system integrity;
- operational management, including service continuity;

[2] Law Decree No. 105 of September 21, 2019 (converted with amendments, by Law No. 133 of November 18, 2019) established the PSNC. Several implementing decrees have been adopted since then: *(i)* Italian President of the Council of Ministers' Decree ("**DPCM**") of July 30, 2020, No. 131, which provided the criteria and methods for identifying the entities included in the PSNC; *(ii)* Presidential Decree ("**DPR**") of February 5, 2021, No. 54, which regulates the verification procedures of the security conditions and the absence of vulnerability of ICT assets and services; DPCM of April 14, 2021, No. 81, which defines the notification procedures in the event of incidents involving ICT Assets; *(iii)* DPCM of June 15, 2021, which identifies the categories of ICT assets, systems and services that will be subject to verification of the security conditions and the absence of vulnerability; *(iv)* DPCM of May 18, 2022, No. 92, regarding the identification of the accreditation rules of the laboratories entrusted with the verification of the security conditions and the absence of vulnerabilities of ICT assets, systems and services.

[3] The ACN, established by Law Decree No. 82 of June 14, 2021 (converted, with amendments, by Law No. 109 of August 4, 2021), has different competencies in relation to the PSNC, having taken over all the functions previously attributed to the Ministry of Economic Development, the Prime Minister's Office, the Department of Security Information (DIS) and the CVCN as well as the inspection and enforcement activities and most of those related to the detection of violations and the imposition of administrative penalties.

[4] Failure to submit such list may result in an administrative fine ranging from EUR 200,000 to EUR 1,200,000.

- monitoring, auditing and control;
- training and awareness;
- procurement of ICT assets, systems and services.

The ACN may conduct audits and inspections to verify, among other things, whether security measures have been properly implemented.[5]

Category A security measures

They must be adopted within six months of the date of submission of the lists of ICT Assets.

- Example: the entity included in the PSNC must conduct a risk assessment that includes the identification and documentation of resource vulnerabilities.

Category B security measures

They must be adopted within 30 months of the date of submission of the lists of ICT Assets.

- Example: following the risk assessment, a document should be prepared describing the decisions made with respect to each identified risk and its priority.

Localization requirements[6]

Localization requirements vary depending on the type of data being processed:

- Digital data processed through the use of ICT Assets or relating to the description of ICT Assets. They must be stored, processed or extracted exclusively through the use of physical and technological infrastructures, even if outsourced, located within the national territory. Such infrastructures also include those dedicated to business continuity functions.
- Digital data used by the security and disaster recovery infrastructure. Even if they are outsourced, they must be located within the national territory, unless there are justified and documented regulatory or technical reasons for not doing so. However, if such reasons exist, the aforementioned data and infrastructure may not be located outside the territory of the European Union.
- Backup digital data. If encrypted, even if outsourced, it may be stored outside the national territory, but not outside the territory of the European Union, and the encryption keys must be kept within the national territory. Encryption and decryption operations must be performed by infrastructure located within the national territory.

These localization requirements are probably the most difficult to apply in practice, as they may require a significant restructuring of the architecture of information systems.

The localization of data and of the physical and technological infrastructure useful for its processing is intended to facilitate:

- the verification of the implementation of security measures, including through physical on-site inspections by Italian authorities;
- the verification and evaluation of possible causes in the event of incidents;
- the shortening of the data control chain;
- greater flexibility in the modification of specific security measures.

Therefore, it is a tool that aims to make the processing of relevant data controllable and measurable, including by facilitating the interaction between the controlled entity and the controlling entity in the event of incidents that threaten national security.

Notification of security incidents

[5] Failure to comply with this obligation may result in an administrative fine ranging from EUR 250,000 to EUR 1,500,000.

[6] DPCM of April 14, 2021, No. 81, Annex B, Article 3.3.1 PR.DS-1.

When an entity included in the PSNC becomes aware of an event described in Annex A of DPCM No. 81/2021, it must notify CSIRT Italia, through the appropriate channels. There is also the possibility of voluntary notification of incidents not specified in the regulatory framework, which in any case cannot have the effect of imposing on the notifying party obligations such party would not have been subject to if it had not voluntarily made the notification.

Notification must be made within six hours in the case of an incident listed in Table 1 of Annex A (*e.g.*, evidence of unauthorized use of techniques that can be used to exfiltrate data from within the network to external resources), and within one hour in the case of an incident listed in Table 2 of Annex A (*e.g.*, unauthorized disclosure of digital data related to ICT Assets).[7] The deadlines run from the time the entities included in the PSNC become aware of the incident.

With regard to incidents that do not affect ICT Assets, and that fall under one of the categories indicated in Annex A of the Resolution,[8] notification is mandatory for incidents falling under the categories listed in Section 1 of Annex A, while it is voluntary (and may be made in the same manner as for the mandatory notification) for incidents listed in Section 2. The notification of these incidents must be sent to CSIRT Italia within 72 hours of the time the affected party becomes aware of them, after having obtained evidence also through monitoring, testing and control activities.

In order to unambiguously identify these terms, one of the security measures described in Annex B of DPCM No. 81/2021 requires that the entities included in the PSNC develop a document identifying the roles, processes and responsibilities for the activities preparatory to the detection of impact incidents and their subsequent notification to CSIRT Italia as well as elements aimed at ensuring the timely detection of such events.

Once the plans for the implementation of the activities for the remediation of the ICT Assets affected by the notifiable incident have been defined and put in place, the entity included in the PSNC must immediately notify CSIRT Italia. If requested by CSIRT Italia and within thirty days of such request, the entity included in the PSNC must also provide a technical report describing the essential elements of the incident, including the consequences of the impact on the ICT Assets resulting from the incident and the remediation actions taken, unless the prosecuting judicial authority has previously communicated the existence of specific needs for investigative secrecy.

II. The procedure before the CVCN

Entities included in the PSNC are required to submit a notification to the CVCN when they intend to proceed with the procurement of ICT assets, systems and services falling within the categories identified by the DPCM of June 15, 2021, and intended for use on ICT Assets.[9]

The notification includes, among other things, a document analyzing the risk associated with the subject matter of the supply.[10]

Timing

- Entities included in the PSNC must notify the CVCN before initiating procurement

[7] Failure to comply with the notification requirement may result in an administrative fine ranging from EUR 250,000 to EUR 1,500,000.

[8] The Resolution classifies cyber incidents and the various phases of the attack into six categories (divided between Section 1, which covers the categories of initial access, execution, installation, lateral movement, and actions on targets, and Section 2, which covers spearphishing activity), and provides an identification code for each incident, along with a description of each type. The incidents listed in the Resolution include most of the cyber attack techniques described by the MITRE ATT&CK, an international reference for cyber attack techniques and procedures (accessible through the following link).

[9] Article 1(6) of D.L. No. 105/2019. These categories include: hardware and software components that perform telecommunications network functions and services (access, transport, switching), such as routers; hardware and software components that perform functions for the security of telecommunications networks and the data they process, such as virtual private networks (VPN); hardware and software components for data acquisition, monitoring, supervisory control, implementation, and automation of telecommunications networks and industrial and infrastructure systems, *e.g.*, AI and ML systems for network or system management; and software applications for implementing security mechanisms, such as single sign-on applications.

[10] The use of products and services on networks that do not comply with the conditions or do not pass the tests imposed by the CVCN may result in an administrative fine ranging from EUR 300,000 to EUR 1,800,000. Failure to comply with the requirements imposed by the CVCN may also result in an administrative fine ranging from EUR 250,000 to EUR 1,500,000.

procedures or signing contracts for the provision of ICT assets, systems and services.

- From the date of the notification, the CVCN has a period of forty-five days (extendable once by fifteen days in cases of particular complexity) to carry out preliminary checks and, if necessary, to request information.
- A subsequent period (of sixty days) is foreseen for the performance of the tests ordered by the CVCN at the end of the preliminary verifications, starting from the time when the entity included in the PSNC, which has been ordered by the CVCN to perform the tests, notifies that the asset to be evaluated has been made physically available for these tests.
- The terms of the procedure may be suspended if the CVCN requests information from the entity included in the PSNC and the information provided is incomplete or inconsistent, or if there is a malfunction of the evaluation object or the test environment set up by the supplier that makes it impossible or difficult to perform the tests.

The tests that the CVCN may require are:

- proper implementation testing of security features in order to verify that they operate according to their respective design specifications; and
- intrusion testing to support vulnerability analysis.

The CVCN may require compliance with specific conditions and tests to be performed and may impose additional requirements regarding the support to be offered by the provider, including that the contract between the provider and the entity included in the PSNC be amended to make it contingent upon compliance with the requirements and the positive outcome of the tests.[11]

It is important that the timing of the procedure before the CVCN is contractually regulated (e.g. through conditions precedent and/or commitments to incorporate the requested changes into the contract) since the notification to the CVCN must be made "*prior to the signing of contracts*", but the timing of the procedure is not entirely predictable.

III. Obligations on providers

There are specific obligations on the provider that supplies relevant assets or services to parties included in the PSNC.

With regard to the implementation of security measures by entities included in the PSNC, the provider must:

- enable the entity included in the PSNC to assess its technical reliability based on a cyber supply chain risk assessment process (including the quality of cybersecurity products and practices, the ability to ensure procurement, support and maintenance over time, and the willingness to share source code, the existence of certifications or evidence useful for assessing the quality of the software development process, the implementation of procedures and technical tools to ensure the authenticity and integrity of software or firmware installed in ICT Assets, and the implementation of procedures and technical tools to ensure a unique match between source code and object code installed and executed within ICT Assets);
- implement appropriate measures to achieve the objectives of the cybersecurity program and risk management plan related to the cyber supply chain adopted by the entity included in the PSNC;
- allow the entity included in the PSNC to conduct audits, reviews, or other forms of periodic evaluation to confirm compliance with contractual obligations.

[11] Article 5(6) of DPR No. 54 of February 5, 2021.

Also with respect to the process before the CVCN, the regulatory framework imposes specific obligations on the provider, including to:

- provide the CVCN with evidence of the suitability of the security features and their configurations to meet the security requirements;
- set up a test environment at a LAP or, if necessary, at the headquarters of the provider or entity included in the PSNC;
- provide a general description of the architecture of the ICT services, assets or systems under evaluation and their functions;
- provide a description of the security features implemented with respect to the ICT services, assets or systems under evaluation;
- provide a description of the functional and security tests already performed, including their results;
- cooperate with the CVCN in the performance of the tests and take action to resolve any malfunctions.

The costs of the evaluation activities performed by the CVCN and the testing activities performed by the LAP are borne by the provider.

Contractual obligations

Contracts with vendors providing relevant assets or services to entities included in the PSNC may regulate additional aspects such as, for example, time frame and manner in which:

- the entity included in the PSNC performs audit activities on the provider; and
- communication between the parties takes place in the event of security incidents.

IV. Conclusions

The PSNC should be conceived as a dynamic regulatory framework that is constantly being updated due to the rapidly evolving nature of cyber risks, both in terms of the obligations imposed on the entities included in the PSNC, in particular with regard to security measures, and in terms of the list of entities included.

In addition, this framework is also of particular relevance to providers of assets and services which, although not included in the PSNC, are the direct recipients of specific obligations and must ensure that their offerings comply with the obligations to which their customers included in the PSNC are subject.

...

CLEARY GOTTLIEB