FÖRSVARSMAKTEN Säkerhetspolisen

240205 **Appendix B2**

Consultation with the Swedish Post and Telecom Authority (PTS) on the licensing of spectrum bands – general procedure

Introduction

In matters relating to licenses to use radio transmitters, the Swedish Post and Telecom Authority (PST) must consult with the Swedish Security Service and the Swedish Armed Forces to assess whether the granting of such licences can be assumed to have the potential to cause harm to Sweden's security.

In their assessment, the Swedish Security Service and the Swedish Armed Forces (hereinafter *the consulting agencies*) will take into account, among other things, the guiding principles previously presented. The consulting agencies will also make a risk assessment in which non-technical vulnerabilities and other potential risks associated with operators and suppliers are taken into consideration.

This document provides a more detailed account of the technical requirements linked to each guiding principle, and the interdependencies between certain principles. The criteria, to be considered by the consulting agencies in the risk assessments linked to each applicant, are also set out in this document.

The new provisions in the Electronic Communications Act (2022:482), concerning the protection of Sweden's security in relation to radio usage, apply to all licensed use of radio transmitters. However, the present document mainly describes the requirements and bases for assessment taken into account by the consulting agencies when reviewing each application submitted in accordance with the *Open invitation part 1 to apply for licences to use radio transmitters in parts of the 1800 MHz-band.*

Should operators, as part of their applications, submit documentation containing classified information, this will be handled in compliance with applicable legislation.

Principles for electronic communication networks critical to Sweden's security, and for suppliers of such networks

For the consulting agencies, the guiding principles form a basis for how suppliers of critical electronic communication networks must design their networks to ensure the protection of Sweden's security. In this context, this mainly concerns network functionality and communication services provided by the operator to the end-user.

The first eleven principles mainly concern technical and procedural requirements. The remaining five principles describe how operators shall meet requirements regarding oversight, control and overall security measures, including protective security measures.

Each principle sets unique requirements in relation to the overall functionality of the networks, and the requirements set out in some principles must be met in order to meet the requirements of other principles. The overall description of systems architecture must therefore indicate how

the requirements of each principle will be met. A brief outline of what the consulting agencies will take into consideration in their assessments follows below. An account of how each principle will be complied with must accompany the application. Should one or several principles be complied with, in whole or in part, by means of international standards, a reference to the relevant standard(s) must be provided.

Operators are expected to apply all principles in their contacts with, and in their specifications of requirements to, suppliers and subcontractors of hardware/software, and as regards operation and maintenance.

Central functions are here to be understood as functions in the radio access network, the core network, the transmission networks, and the operation and maintenance network that are necessary to maintain overall network functionality and electronic communication services provided by the operator to the end-user, as well as regulatory services (such as the emergency number in Sweden 112).

1. Must function even if international connections are cut off

Description:

The operator must demonstrate that central functions operate on a continuous basis within Sweden and are not dependent on international connections.

On a more general level, this principle relates to accessibility, as described in more detail in principle 3.

The operator must have a clear plan for ensuring network functionality in the event of disruptions associated with products or suppliers. The operator must also have a clear plan for managing security incidents from Sweden, and for storing systems and user data in Sweden.

2. Must provide functions allowing for simple, swift and selective cutting off of connections to and from other countries

Description:

The operator must account for connection points to other countries, their function and how the cutting off of connections is handled.

Principles 1 and 2 are interdependent in that the cutting off of connections to and from other countries would otherwise make the network go down or significantly impair its functionality.

The operator must have a clear plan for ensuring network functionality in the event of disturbances or cyber-attacks from other countries. The operator must also specify how influencing attempts by other countries will be prevented, e.g. by making tools for monitoring network traffic inaccessible from other countries.

3. Must provide a high level of accessibility and confidentiality

Description:

The operator must specify which functions are considered critical in terms of accessibility and confidentiality, and which protective measures are taken to safeguard these functions.

Principles 3 and 4 are in part interdependent in that the requirements set out in principle 3 cannot be met unless the operator has 'requisite oversight and control' (principle 4).

The operator must account for how the networks for e.g. administration, authorisation, operation, maintenance, control and environmental management, and associated data, are protected and separated from other networks such as the internet, the operator's traffic plan and enterprise networks, and other networks connected to the internet.

The operator must account for how they manage risks associated with the control and signalling plan.

The operator must demonstrate that the implementation of virtualisation layers is done in such a way that it will secure accessibility and confidentiality across the network, including, but not limited to, its configuration and life cycle management.

4. Must allow for requisite oversight and control

Description:

The operator must account for how its systems architecture and processes minimise the risk of network components being used for monitoring and manipulation, including e.g. an account of tools and processes for monitoring and identifying network traffic, and interfaces to administrative functions (both physical and logical).

The operator must also account for how oversight and control are exercised in relation to suppliers and their subcontractors.

Principles 4 and 5 are in part interdependent in that the operator cannot be assumed to have 'requisite oversight and control' unless they can prevent 'unauthorised control'. Principle 4 is also in part dependent on principle 9 in that access control is necessary for the implementation of principle 4.

5. Must be designed to prevent unauthorised control and manipulation

Description:

The operator must account for the measures taken to protect critical network functions against unauthorised control and manipulation, e.g. by separating administration and signalling, and by using traffic protection.

The operator must also account for how the above is applied in relation to suppliers and their subcontractors.

Principle 5 primarily depends on principles 3 (accessibility) and 4 (requisite oversight and control).

6. Must be designed to prevent control and manipulation from abroad

Description:

This principle sets out additional requirements to those described under principle 5. In similarity with principle 1, the operator must demonstrate that central network functions are located in Sweden and cannot be controlled or manipulated from abroad.

7. Must be designed to prevent unauthorised access to information on services, capacity, locations and users

Description:

Services, in this context, refer not only to central network functions but also to communication services provided by operators to end-users, and regulatory services provided by operators (such as Sweden's emergency number 112).

The operator must account for the configuration of both its physical and virtualised infrastructure, not only to ensure network security but also to prevent unauthorised access to information (such as espionage or other intelligence activities) targeting central network functions and user data. In this context, the operator must also account for their protection of databases

containing user data, including locations data, and information regarding which services are used and their capacity.

The operator must also account for how the above is implemented in relation to suppliers and their subcontractors.

Principle 7 adds further requirements in relation to all other principles.

8. ***Must be designed to withstand hostile attacks (e.g. electronic attacks) and, where this is not possible, such attacks must be detected and prevented***

Description:

The operator must account for measures taken to secure functions used to identify, protect, detect and counter cyber-attacks or other electronic attacks, and to restore functionality.

The operator must also account for how the above is implemented in relation to suppliers and their subcontractors.

Principle 8 adds further requirements in relation to all other principles.

9. ***Must have access control systems for functions that may affect confidentiality, accessibility, oversight and control***

Description:

The operator must account for the access control systems used in relation to the central functions. This includes e.g. describing how authorisations are designed and implemented in the virtual infrastructure, and procedures for the issuing and life cycle management of authorisations. The operator is expected to have adequate procedures for ensuring uninterrupted operation of access control systems that are developed as the network develops.

The operator must also account for how the above is applied in relation to suppliers and their subcontractors. It is of particular importance that policies for authorisation consider risks associated with external access by third parties, and how such risks will be minimised.

Principle 9 primarily depends on principle 5 (prevent unauthorised control).

10. ***Must have traceability for functions that may affect confidentiality, accessibility, oversight or control***

Description:

The operator must account for both physical and virtual devices connected to central network functions, and describe systems and procedures for logging, log analysis and security audit. This also applies to third-party activities.

Principle 10 primarily depends on principle 9 (access control systems).

11. ***Must be designed in a way to ensure that equipment involving a risk of unauthorised access, control or manipulation through physical access is located on Swedish territory, thereby ensuring applicability of Swedish law***

Description:

The operator must demonstrate that central network functions are located on Swedish territory (cf. principle 1). The operator is also required to manage security incidents from Sweden, and systems and user data must be stored in Sweden.

12. ***The operator must continuously provide designated recipients at sector-specific oversight agencies with information on measures taken in communication networks and which may affect confidentiality, resilience, accessibility, oversight or control***

13. ***The operator must provide this information in a timely manner to enable sector-specific oversight agencies to determine which risks such measures could entail and whether any action needs to be taken***

14. ***The operator must actively facilitate oversight and inspection by sector-specific oversight agencies***

Description of principles 12, 13 and 14:

The operator must describe a model and a procedure for their sharing of information on central functions with the oversight agencies.

The operator must also account for how the above is applied in relation to suppliers and their subcontractors.

15. ***The operator must develop, implement, operate and maintain adequate protective security measures***

Description:

This principle concerns the overall assessment of the operator's security solutions, including their protective security measures.

The operator must account for their overall security architecture, including the level of network integration, flexibility and automation, as well as administrative security measures in relation to different security solutions. The links to the relevant principles (1-11) must be clearly stated.

The operator must also account for how the above is applied in relation to suppliers and their subcontractors.

16. ***The operator must ensure that personnel given access to information that may affect confidentiality, integrity, resilience and accessibility are approved, have received protective security training and are aware of the confidentiality of this information***

Description:

This principle concerns the overall assessment of the operator's protective security measures in relation to personnel and information security.

Assessment criteria

In their assessments, and in addition to the principles described above, the consulting agencies will consider non-technical vulnerabilities and other potential risks associated with operators, suppliers and subcontractors.[1] Among the criteria to be considered by the consulting agencies are:

- The likelihood that an operator or supplier is subject to influencing attempts/unlawful pressure. Such influencing attempts/unlawful pressure may be aided by, but are not limited to, the existence of the following criteria:
    - Links, including ownership and other links, to a government or a government agency in a third country (non-EU member state).
    - The legislation of a third country, especially where there are no legislative or democratic checks and balances in place, or in the absence of security or data protection agreements.
    - Links to countries or organisations involved in cyber operations or other antagonistic activities against Sweden.
    - Other possibilities for a third country to exercise any form of pressure, e.g. in relation to the place of manufacturing of the equipment.

- The supplier's ability to assure the supply of critical products.

ENDS

[1] cf. NIS Cooperation Group. CG Publication 01/2020. *Cybersecurity of 5G networks EU Toolbox of risk mitigating measures*