18.1. Network Management

Objective

18.1.1. Any change to the configuration of networks is authorised and controlled through appropriate change management processes to ensure security, functionality and capability is maintained.

Context

Scope

18.1.2. This section covers information relating to the selection, management and documentation of network infrastructure.

Network diagrams

18.1.3. An agency's network diagrams should illustrate all network devices including firewalls, IDSs, IPSs, routers, switches, hubs, etc. It does not need to illustrate all IT equipment on the network, such as workstations or printers which can be collectively represented. The inclusion of significant devices such as MFD's and servers can aid interpretation.

Systems Documentation

18.1.4. Knowledge of systems design, equipment and implementation is a primary objective of those seeking to attack or compromise systems or to steal information. System documentation is a rich source allowing attackers to identify design weaknesses and vulnerabilities. The security of systems documentation is therefore important in preserving the security of systems.

18.1.5. Detailed network documentation and configuration details can contain information about IP addresses, port numbers, host names, services and protocols, software version numbers, patch status, security enforcing devices and information about information compartments and enclaves containing highly valuable information. This information can be used by a malicious actor to compromise an agency's network.

18.1.6. This information may be particularly exposed when sent to offshore vendors, consultants and other service providers. Encrypting this data will provide an important protective measure and assist in securing this data and information.

18.1.7. Reference should also be made to Section 12.7 – Supply Chain.

PSR references

18.1.8. Relevant PSR requirements can be found at:

Reference	Title	Source
PSR Mandatory Requirements	GOV5, GOV6, INFOSEC1, INFOSEC2, INFOSEC3 and INFOSEC4	Home | Protective Security Requirements Security governance (GOV) | Protective Security Requirements Information security (INFOSEC) | Protective Security Requirements/

Rationale & Controls

Classification of Network Documentation

18.1.9.R.01. **Rationale**

To provide an appropriate level of protection to systems and network documentation, a number of security aspects should be considered. These include:

- the existence of the system;
- the intended use;
- the classification of the data to be carried or processed by this system;
- the connectivity and agencies connected;
- protection enhancements and modifications; and
- the level of detail included in the documentation.

High level conceptual diagrams and accompanying documentation should also be subject to these considerations

18.1.9.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3170]

Agencies MUST perform a security risk assessment before providing network documentation to a third party, such as a commercial provider or contractor.

18.1.9.C.02. **Control System Classifications(s): Secret, Confidential, Top Secret; Compliance: Must** [CID:3172]

Systems documentation and detailed network diagrams MUST be classified at least to the level of classification of the data to be carried on those systems.

18.1.9.C.03. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3174]

Network documentation provided to a third party, such as to a commercial provider or contractor, MUST contain only the information necessary for them to undertake their contractual services and functions, consistent with the need-to-know principle.

18.1.9.C.04. **Control System Classifications(s): All Classifications; Compliance: Must Not** [CID:3176]

Detailed network configuration information MUST NOT be published in tender documentation.

18.1.9.C.05. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3179]

Security aspects SHOULD be considered when determining the classification level of systems and network documentation.

Configuration management

18.1.10.R.01. **Rationale**

If the network is not centrally managed, there could be sections of the network that do not comply with the agency's security policies, and thus create a vulnerability.

18.1.10.R.02. **Rationale**

Changes should be authorised by a change management process, including representatives from all parties involved in the management of the network. This process ensures that changes are understood by all parties and reduces the likelihood of an unexpected impact on the network.

18.1.10.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3188]

Agencies SHOULD keep the network configuration under the control of a network management authority.

18.1.10.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3190]

All changes to the configuration SHOULD be documented and approved through a formal change control process.

18.1.10.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3191]

Agencies SHOULD regularly review their network configuration to ensure that it conforms to the documented network configuration.

18.1.10.C.04. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3192]

Agencies SHOULD deploy an automated tool that compares the running configuration of network devices against the documented configuration.

Network diagrams

18.1.11.R.01. **Rationale**

As most decisions are made on the documentation that illustrates the network, it is important that:

- a network diagram exists;
- the security architecture is recorded;
- the network diagram is an accurate depiction of the network; and
- the network diagram indicates when it was last updated.

18.1.11.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3195]

For each network an agency manages they MUST have:

- a high-level diagram showing all connections and gateways into the network; and
- a network diagram showing all communications equipment.

Updating network diagrams

18.1.12.R.01. **Rationale**

Because of the importance of the network diagram and decisions made based upon its contents, it should be updated as changes are made. This will assist system administrators to completely understand and adequately protect the network.

18.1.12.C.01. **Control System Classifications(s): Secret, Top Secret, Confidential; Compliance: Must** [CID:3198]

An agency's network diagrams MUST:

- be updated as network changes are made; and
- include a 'Current as at [date]' statement on each page.

18.1.12.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3199]

An agency's network diagrams SHOULD:

- be updated as network changes are made; and
- include a 'Current as at [date]' statement on each page.

Limiting network access

18.1.13.R.01. **Rationale**

If an attacker has limited opportunities to connect to a given network, they have limited opportunities to attack that network. Network access controls not only prevent against attackers traversing a network but also prevent system users carelessly connecting a network to another network of a different classification. It is also useful in segregating sensitive or compartmented information for specific system users with a need-to-know.

18.1.13.R.02. **Rationale**

Although circumventing some network access controls can be trivial, their use is primarily aimed at the protection they provide against accidental connection to another network.

18.1.13.R.03. **Rationale**

The design of a robust security architecture is fundamental to the security of a system. This may include concepts such as trust zones, application of the principles of separation and segregation through, for example, segmented networks and VPNs and other design techniques.

18.1.13.C.01. **Control System Classifications(s): Top Secret, Secret, Confidential; Compliance: Must** [CID:3204]

Agencies MUST implement network access controls on all networks.

18.1.13.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3205]

Agencies SHOULD implement network access controls on all networks.

Management traffic

18.1.14.R.01. **Rationale**

Implementing protection measures specifically for management traffic provides another layer of defence on the network. This also makes it more difficult for an attacker to accurately define their target network.

18.1.14.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3208]

Agencies SHOULD implement protection measures to minimise the risk of unauthorised access to network management traffic on a network.

Simple Network Management IT Protocol (SNMP)

18.1.15.R.01. **Rationale**

The Simple Network Management Protocol (SNMP) can be used to monitor the status of network devices such as switches, routers and wireless access points. Early versions of SNMP were insecure. SNMPv3 uses stronger authentication methods but continues to establish default SNMP community strings and promiscuous access. Encryption may be used as an additional assurance measure but this may create additional workload in investigating faults. An assessment of risk, threats and the agency's requirements may be required to determine an appropriate configuration.

18.1.15.C.01. **Control System Classifications(s): All Classifications; Compliance: Should Not** [CID:3211]

Agencies SHOULD NOT use SNMP unless a specific requirement exists.

18.1.15.C.02.

Control System Classifications(s): All Classifications; Compliance: Should [CID:3238]

Agencies SHOULD implement SNMPv3 where a specific SNMP requirement exists.

18.1.15.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3239]

Agencies SHOULD change all default community strings in SNMP implementations.

18.1.15.C.04. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3240]

SNMP access SHOULD be configured as read-only.