Documents required for the UPU security standards

1 Risk assessment (S58 section 5.1.1) – provide copies of the two most recent risk assessment reports.

An annual risk assessment shall be conducted to identify each critical facility. The assessment shall take into consideration the postal assets and operations at the facility, the general crime rate of the area and other contributing factors that increase the likelihood of criminal incidents.

2 Critical facility security plans (S58 section 5.1.1) – provide a copy of the security plan for each critical facility.

For each critical facility, a detailed written security plan shall be developed and maintained. The security plan shall contain the following control measures:

i critical facility design standards;

ii perimeter barriers;

iii perimeter windows, doors or other openings;

iv lighting;

v locking mechanisms and key controls;

vi access control measures.

3 Critical facility design standards (S58 section 5.1.2) – provide copies of the documented annual inspection programme plan and the two most recent inspection reports. If repairs were carried out, provide copies of the repair records for the last two inspection reports.

A designated programme of annual inspection and repair shall be conducted to assure the integrity of structures including timescales for completion of any repair.

4 Perimeter barriers (S58 section 5.1.3) – provide the last two weekly perimeter inspection reports.

Weekly inspections of the perimeter barriers shall be conducted to ensure their integrity.

5 Locking mechanisms and key controls (S58 section 5.1.6) – provide the key issuance record or register (log).

A key control system shall be maintained for adequate key accountability. The system shall register and record the issuance of keys and protect access to non-issued keys. The key control system shall be administered by the Postal Security Unit or the respective postal facility manager.

6 Access control systems for employees, visitors, service providers and vendors (S58 section 5.2.2) – if a manual access control system or process is in place, please provide documentation.

A visitor registration system shall be implemented to record entries of non-employees into secure areas of the critical facility.

7 Personnel security and hiring processes (S58 section 6.2) – please provide a copy of the hiring or personnel selection policy.

The personnel selection and hiring policy shall be documented for all employees working within the facilities of the designated operator (DO) or handling mail at external locations. The hiring policy shall be consistent with national legislation to ensure prospective and current employees and contractors are qualified to perform postal duties as a person of integrity. Background checks (criminal history or police checks) for all career

employees shall be conducted consistent with national legislation. A process shall be maintained to report and communicate employee performance and misconduct. The hiring process shall include interviews, pre-employment data verification and other confirmation measures commensurate with positions or duties. The termination process shall be documented for employees and contractors. The termination process shall ensure the timely return of identification documents, access control devices, keys, uniforms and other sensitive information. A record system shall be maintained to prevent re-hiring of employees or contractors who have been terminated due to misconduct.

8 Awareness and training measures (S58 section 6.4) – please provide a copy of security awareness programmes.

Security awareness training programmes shall be documented and maintained for all employees and contractors.

9 Transportation and conveyance security requirements for DOs and postal contractors (S58 section 7) – please provide a copy of the documented process for security of the mail by all modes (air, road, sea and rail) of transportation.

The DO and authorized contractors shall document processes and procedures for security of the mail by all modes (air, road, sea and rail) of transportation. The DO shall comply with all applicable national legislation regarding transportation standards.

Vehicle cabin and ignition keys for all transport vehicles shall be secured from unauthorized access. A key accountability process shall be maintained.

Routes, schedules and planned stops shall be assessed for risk and, if necessary, an additional security measure shall be initiated to mitigate the risk.

10 Compliance audit programme and oversight (S58 section 8) – please provide the most recent report of the annual compliance audit of the mail security programme.

An annual compliance audit shall be conducted by personnel independent of the critical facility management team.

The compliance audit review programme covers the entire mail security programme to ensure implementation of security requirements. The compliance audit review programme shall include, but not be limited to, an emphasized focus on:

– facility security;

– personnel security;

– transportation and conveyance security.

The DO shall ensure that the management of the compliance audit review programme is independent from individuals responsible for the implementation of security requirements. Records of the compliance audits and recommendations shall be maintained. The result of the compliance audits shall be reported to the executive management of the DO. Follow-up actions shall be monitored and documented.

11 Postal security unit for prevention and investigative management (minimum security requirement) (S58 section 9.1) – please provide a copy of the security programme covering the areas of prevention and investigation for the protection of mail, employees, partners, customers and postal assets, as well as a copy of the DO's organizational structure.

The DO shall have a documented security programme covering the areas of prevention and investigation for the protection of mail, employees, partners, customers and postal assets. This shall be communicated to all employees.

12 Disaster recovery, emergency preparedness and business continuity planning (S58 section 9.2) – please provide copies of the crisis and business continuity plans.

The DO shall document and communicate to appropriate employees:

– a crisis plan to ensure the security of mail, employees, customers and postal assets in the event of a man-made or natural disaster that would affect the flow of mail or postal operations;

– a business continuity plan to minimize postal interruption in the event of significant incident which might impact domestic or international postal operations.