Date of review:_____ Name of facility:_____ Reviewer:_____

Standard	Sect.	Section name	Sub-section	Requirement (standard language)	On site or pre-assessment	Question to:	Question	Response
S58	5.1.1	Risk assessment and critical facility security plans	5.1.1.1	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.	Both on site and pre-assessment	DO security	Do you conduct an annual risk assessment for each critical facility (the office of exchange is one critical facility, but you may have more)? If so, would you please provide two recent risk assessment reports for our review?	
S58	5.1.1	Risk assessment and critical facility security plans	5.1.1.2	For each critical facility, a detailed written security plan shall be developed and maintained. The security plan shall contain the following control measures: • critical facility design standards; • perimeter barriers; • perimeter windows, doors or other openings; • lighting; • locking mechanisms and key controls; • access control measures.	Both on site and pre-assessment	DO security	Do you have a written facility security plan for each critical facility? If yes, provide a copy of the facility security plan for each critical facility.	
S58	5.1.2	Critical facility design standards	5.1.2.2	A designated programme of annual inspection and repair shall be conducted to assure the integrity of structures.	Both on site and pre-assessment	DO security	Do you conduct a programme of annual inspection and repair to assure the integrity of facility structures? If so, please provide copies of the documented programme plan and two most recent inspection reports.	
S58	5.1.2	Critical facility design standards	5.1.2.2	A designated programme of annual inspection and repair shall be conducted to assure the integrity of structures.	Both on site and pre-assessment	DO operations	Have you conducted repairs based on inspection report? If yes, please provide copies of the repair records for the last two inspection reports?	
S58	5.1.3	Perimeter barriers	5.1.3.2	Weekly inspections of the perimeter barriers shall be conducted to ensure their integrity.	Both on site and pre-assessment	DO security	Do you conduct weekly inspections of the perimeter barriers? If yes, please provide the last two weekly inspection reports?	
S58	5.1.6	Locking mechanisms and key controls	5.1.6.2	Key controls A key control system shall be maintained for adequate key accountability. The system shall be administered by the postal security unit or the respective postal facility manager. The system registers and records the issuance of keys and protects access to non-issued keys through the maintenance of a locked key storage location.	Both on site and pre-assessment	DO security	Do you have a key control system? If so, please describe.	

Standard	Sect.	Section name	Sub-section	Requirement (standard language)	On site or pre-assessment	Question to:	Question	Response	
S58	5.1.6	Locking mechanisms and key controls	5.1.6.2	Key controls A key control system shall be maintained for adequate key accountability. The system shall be administered by the postal security unit or the respective postal facility manager. The system shall register and record the issuance of keys and protect access to non-issued keys through the maintenance of a locked key storage location.	Both on site and pre-assessment	DO security	Is someone clearly designated as responsible for maintaining the key control system? Who?		
S58	5.1.6	Locking mechanisms and key controls	5.1.6.2	Key controls A key control system shall be maintained for adequate key accountability. The system shall be administered by the postal security unit or the respective postal facility manager. The system shall register and record the issuance of keys and protect access to non-issued keys through the maintenance of a locked key storage location.	Both on site and pre-assessment	DO security	Does the key control system register and record the issuance of keys? If yes, provide the key issuance record or register (log).		
S58	5.1.6	Locking mechanisms and key controls	5.1.6.2	Key controls A key control system shall be maintained for adequate key accountability. The system shall be administered by the postal security unit or the respective postal facility manager. The system shall register and record the issuance of keys and protect access to non-issued keys through the maintenance of a locked key storage location.	Both on site and pre-assessment	DO security	Are non-issued keys protected in a locked key storage location?		
S58	5.2.1	Access control measures: General	5.2.1.1	Levels of access control: Access control measures shall prevent unauthorized access to mail - and mail conveyance vehicles - in critical facilities. The appropriate level of access control shall be implemented at every critical facility to protect and secure postal assets. *NOTE: Access control may be a manual process utilizing fixed security guard posts at entry/egress points to verify the identity of the individual or vehicle entering the secure area. Access control measures may also consist of simple or complex electronic systems to verify and permit access to the secure areas. Regardless of the technological aspects of the methods utilized, the system must possess the ability to adequately screen and differentiate the access privileges of employees, visitors, service providers and vendors at all points of entry. The access control system in a critical facility is segmented to ensure that employees, visitors, service providers and vendors be only permitted access to those areas of a facility where they have work functions or conduct business.*	Both on site and pre-assessment	DO security	How do the access control measures implemented prevent unauthorized access to mail and mail conveyance vehicles in critical facilities?		

Standard	Sect.	Section name	Sub-section	Requirement (standard language)	On site or pre-assessment	Question to:	Question	Response	
S58	5.2.1	Access control measures: General	5.2.1.1	Levels of access control: Access control measures shall prevent unauthorized access to mail - and mail conveyance vehicles - in critical facilities. The appropriate level of access control shall be implemented at every critical facility to protect and secure postal assets. *NOTE: Access control may be a manual process utilizing fixed security guard posts at entry/egress points to verify the identity of the individual or vehicle entering the secure area. Access control measures may also consist of simple or complex electronic systems to verify and permit access to the secure areas. Regardless of the technological aspects of the methods utilized, the system must possess the ability to adequately screen and differentiate the access privileges of employees, visitors, service providers and vendors at all points of entry. The access control system in a critical facility is segmented to ensure that employees, visitors, service providers and vendors be only permitted access to those areas of a facility where they have work functions or conduct business.*	Both on site and pre-assessment	DO security	Is the appropriate level of access control implemented at every critical facility to protect and secure postal assets? What type of access control is used?		
S58	5.2.1	Access control measures: General	5.2.1.1	Levels of access control: Access control measures shall prevent unauthorized access to mail - and mail conveyance vehicles - in critical facilities. The appropriate level of access control shall be implemented at every critical facility to protect and secure postal assets. *NOTE: Access control may be a manual process utilizing fixed security guard posts at entry/egress points to verify the identity of the individual or vehicle entering the secure area. Access control measures may also consist of simple or complex electronic systems to verify and permit access to the secure areas. Regardless of the technological aspects of the methods utilized, the system must possess the ability to adequately screen and differentiate the access privileges of employees, visitors, service providers and vendors at all points of entry. The access control system in a critical facility is segmented to ensure that employees, visitors, service providers and vendors be only permitted access to those areas of a facility where they have work functions or conduct business.*	Both on site and pre-assessment	DO security	Is the access control system in a critical facility segmented to ensure that employees, visitors, service providers and vendors are permitted access only to those areas of a facility where they conduct business or have a work related need for entry?		

Standard	Sect.	Section name	Sub-section	Requirement (standard language)	On site or pre-assessment	Question to:	Question	Response	
S58	5.2.2	Access control systems for employees, visitors, service providers and vendors	5.2.2.1	An adequate access control process shall be in place for secure (non-customer) areas of all critical postal facilities. (The system may be manual or automated. Different sections of the standard apply depending on the type of system. Characterize this practice based on whether one type or the other is implemented. Use the remaining sections to characterize the conformance of the system based on its type.)	Pre-assessment	DO security	Is the access control process for the secure (non-customer) areas of all postal facilities automated or manual?		
S58	5.2.2	Access control systems for employees, visitors, service providers and vendors	5.2.2.2	Manual access control: preventing unauthorized entry a. manual access control system ii. uniformed security guards, a receptionist or other personnel staff shall be at entry/egress points to verify the entry privileges for each individual. *Note 1: The carriage of personal belongings, e.g. bags, and the limitation thereof as well as the institution of search procedures should be considered.*	Both on site and pre-assessment	DO security	IF SYSTEM IS MANUAL: How are entry and egress points protected to prevent unauthorized entry? How are the entry privileges verified for each person entering?		
S58	5.2.2	Access control systems for employees, visitors, service providers and vendors	5.2.2.3	Manual access control: documentation and training ii. the manual process shall be documented in a standard operating procedure; iii. training and instructions shall be provided to the respective personnel administering the system and the individuals stationed at the fixed access control point.	Both on site and pre-assessment	DO security	IF SYSTEM IS MANUAL: Do you have a documented manual access control system or process documented and in place for critical postal facilities? If so, please provide documentation.		
S58	5.2.2	Access control systems for employees, visitors, service providers and vendors	5.2.2.3	Manual access control: documentation and training ii. the manual process shall be documented in a standard operating procedure; iii. training and instructions shall be provided to the respective personnel administering the system and the individuals stationed at the fixed access control point.	Both on site and pre-assessment	DO security	IF SYSTEM IS MANUAL: Are training and instructions provided to the respective personnel administering the system and the individuals stationed at the fixed access control point?		
S58	5.2.2	Access control systems for employees, visitors, service providers and vendors	5.2.2.4	Manual access control: visitors and vendors iv. a registration system shall be maintained to record entries of non-employees into secure areas of the critical facility.	Both on site and pre-assessment	DO security	IF SYSTEM IS MANUAL: Are visitors to the facility escorted at all times? Are service providers and vendors escorted? Under what circumstances are vendors and service providers not escorted? (Are unescorted service providers and vendors pre-cleared and/or badged?)		

Standard	Sect.	Section name	Sub-section	Requirement (standard language)	On site or pre-assessment	Question to:	Question	Response	
S58	5.2.2	Access control systems for employees, visitors, service providers and vendors	5.2.2.5	Automated access control: prevent unauthorized entry b. An automated (electronic) access control system The system shall be designed to prohibit unauthorized entries of individuals through the entry/egress points and only through a single access system or process and shall be a single access system to only permit entry for the respective badge holder which activates the access point. *Note 2: A single access system can also be accomplished by assigning a uniformed security guard or other personnel to a fixed post to monitor the entries/egress from the access point. If the entry/egress point is not monitored, physical access control equipment (turnstiles, access gates and doors) activated by badge readers or electronic keys should be used.*	Both on site and pre-assessment	DO security	IF SYSTEM IS AUTOMATED: How are entry and egress points protected to prevent unauthorized entry? Are guards or other personnel posted or is a turnstile or other mechanical means used? Is the system designed so that only a single entry is allowed for the badge holder who activated the system (in other words, how does the system prevent tail-gating)?		
S58	5.2.2	Access control systems for employees, visitors, service providers and vendors	5.2.2.6	Automated access control: visitors and vendors A visitor registration system shall be implemented to record entries of non-employees into secure areas of the critical facility.	Both on site and pre-assessment	DO security	IF SYSTEM IS AUTOMATED: Is a visitor registration system maintained to record entries of non-employees into the secure areas of the critical facility?		
S58	5.2.2	Access control systems for employees, visitors, service providers and vendors	5.2.2.6	Automated access control: visitors and vendors A visitor registration system shall be implemented to record entries of non-employees into secure areas of the critical facility.	Both on site and pre-assessment	DO security	IF SYSTEM IS AUTOMATED: Are visitors to the facility escorted at all times? Are service providers and vendors escorted? Under what circumstances are vendors and service providers not escorted? (Are unescorted service providers and vendors pre-cleared and/or badged?) Are visitors issued electronic access devices? (NOTE: standard requires that visitors NOT be issued such devices)		
S58	5.2.3	Access control systems for vehicles	5.2.3.3	A manual or automated access control system shall be used to ensure unauthorized vehicles do not gain access into the secure exterior operations area.	Pre-assessment	DO security	Is a manual or automated system used to control access to ensure that unauthorized vehicles do not gain access into the secure exterior operations area? If a manual system is used, please be prepared to share documentation on the system.		

Standard	Sect.	Section name	Sub-section	Requirement (standard language)	On site or pre-assessment	Question to:	Question	Response	
S58	5.2.3	Access control systems for vehicles	5.2.3.3	A manual or automated access control system shall be used to ensure unauthorized vehicles do not gain access into the secure exterior operations area.	Pre-assessment	DO security	How is access controlled to ensure unauthorized vehicles do not gain access into the secure exterior operations area? If a manual system is used, please provide documentation on the manual system. If an automated system is used, please provide a demonstration.		
S58	5.2.4	Identification systems	5.2.4.3	The postal security unit or other postal managers shall be responsible for the control, issuance and removal of employee, visitor and contractor identification badges. A process shall be maintained to report and communicate employee information.	Both on site and pre-assessment	DO security	What is the process for the control, issuance and removal of employee, visitor and contractor identification badges? Who is responsible for that process?		
S58	6.1	Personnel security and training: General	6.1.1	General Important to postal operations are its personnel and as such it is fundamental to operators that any potential security risks that are posed as a result of new employees or parties providing services entering into the business, as well as those resulting from the redeployment of employees onto roles with different vetting or training requirements are minimized. Personnel security and training shall be deployed in order to reduce and minimize security risks to the business, its customers and employees.	Both on site and pre-assessment	DO security	This question may also be asked of DO human resources. Is training conducted for new and re-assigned personnel in an effort to minimize security risks to the business, its customers and employees? What is the frequency and type of training conducted?		
S58	6.2	Personnel security and hiring processes	6.2.1	Background checks (criminal history or police checks) for all career employees shall be conducted consistent with national legislation.	Both on site and pre-assessment	DO security	This question may also be asked of DO human resources. Are background checks performed for all career employees consistent with national legislation? How often are they repeated or updated?		
S58	6.2	Personnel security and hiring processes	6.2.1	Employee hiring The personnel selection and hiring policy shall be documented for all employees working within the facilities of the DO or handling mail at external locations.	Both on site and pre-assessment	DO human resources	Do you have a documented personnel selection and hiring policy for employees working within the facilities of the DO or handling mail at external locations? If yes, please provide a copy of the hiring policy for review.		
S58	6.2	Personnel security and hiring processes	6.2.1	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.	Both on site and pre-assessment	DO human resources	Is your selection and hiring policy for employees consistent with national legislation to ensure that people performing postal duties are suitable for the function?		

Standard	Sect.	Section name	Sub-section	Requirement (standard language)	On site or pre-assessment	Question to:	Question	Response	
S58	6.2	Personnel security and hiring processes	6.2.1	The hiring process shall include interviews, pre-employment data verification and other screening measures commensurate with positions or duties.	Both on site and pre-assessment	DO human resources	How are candidate employees evaluated before hiring? Interviews? Verification of pre-employment data? Other checks or measures?		
S58	6.2	Personnel security and hiring processes	6.2.2	The termination process shall be documented for employees and contractors.	Pre-assessment	DO human resources	Do you have a documented termination process? If yes, please be prepared to share the documentation.		
S58	6.2	Personnel security and hiring processes	6.2.2	The termination process shall ensure the timely return of identification documents, access control devices, keys, uniforms and other sensitive information.	Both on site and pre-assessment	DO human resources	Does the termination process ensure the timely return of identification documents, access control devices, keys, uniforms and other sensitive information?		
S58	6.2	Personnel security and hiring processes	6.2.2	A record system shall be maintained to prevent re-hiring of employees or contractors who have been terminated due to misconduct.	Both on site and pre-assessment	DO human resources	Do you have a record system to prevent rehiring employees or contractors who have been terminated for misconduct?		
S58	6.2	Personnel security and hiring processes	6.2.3	A process shall be maintained to report and communicate employee performance and misconduct.	Both on site and pre-assessment	DO human resources	This question may also be asked of DO security. What is the process for reporting and communicating employee performance and misconduct?		
S58	6.3	Contractor security requirements	6.3.1	Contractor compliance Contractors used to perform mail handling/transport operations or other sensitive functions shall apply personnel security measures equivalent to the DO as described in section 6.2.	Pre-assessment	DO operations	Are contractors used to perform mail handling/transport operations or other sensitive functions for the DO? NOTE: If so, then section 6.2 applies. If not, proceed to section 6.4.		
S58	6.3	Contractor security requirements	6.3.2	Contractor security The contractor shall inform the DO of any personnel findings or decisions which could pose a potential security risk to the operation.	Both on site and pre-assessment	DO operations	Question applies if contractors are used. Do contractors inform the DO of any personnel findings or decisions which could pose a potential security risk to the operation?		
S58	6.4	Awareness and training measures	6.4.1	A security awareness training programme shall be documented and maintained for all employees and contractors.	Both on site and pre-assessment	DO security	Do you have a security awareness programme? Is it documented and maintained for all employees and contractors? If yes, please be prepared to share the documentation for review.		

Standard	Sect.	Section name	Sub-section	Requirement (standard language)	On site or pre-assessment	Question to:	Question	Response	
S58	7.1	Transportation and conveyance security requirements for DOs and postal contractors	7.1.1	Documented mail conveyance security procedures 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.	Both on site and pre-assessment	DO security	Do you have a documented process for security of the mail by all modes (air, road, sea and rail) of transportation? Does it also apply to contractors? If yes, please be prepared to provide the documentation for review. Does the DO comply with all applicable national legislation regarding transportation standards?		
S58	7.1	Transportation and conveyance security requirements for DOs and postal contractors	7.1.2	Restricted access to mail Access to mail shall be restricted as appropriate to postal employees or contractors with mail handling responsibilities.	Both on site and pre-assessment	DO security	How is access to mail restricted to postal employees or contractors with mail handling responsibilities?		
S58	7.1	Transportation and conveyance security requirements for DOs and postal contractors	7.1.5	Mail transport vehicle key accountability Vehicle cabin and ignition keys for all transport vehicles shall be secured from unauthorized access. A key accountability process shall be maintained.	Both on site and pre-assessment	DO security	How are vehicle cabin and ignition keys for all transport vehicles secured from unauthorized access? Do you have a key accountability process in place? If so, how is that accountability process maintained and who is responsible for it?		
S58	7.1	Transportation and conveyance security requirements for DOs and postal contractors	7.1.6	Risk assessment of routes Routes, schedules and planned stops shall be assessed for risk and, if necessary, an additional security measure shall be initiated to mitigate the risk.	Both on site and pre-assessment	DO security	Are routes, schedules and planned stops assessed for risk? If yes, what additional security measures are used to mitigate risk?		
S58	8.1	Compliance audit programme and oversight	8.1.1	Annual compliance audits An annual compliance audit shall be conducted by personnel independent of the critical facility management team.	Both on site and pre-assessment	DO security	Is an annual compliance audit conducted on the mail security programme by personnel independent of the management team? Who conducts the audit? Please be prepared to provide the most recent report.		
S58	8.1	Compliance audit programme and oversight	8.1.2	Compliance audit personnel The individuals conducting the compliance audit review shall be afforded the necessary authority to obtain relevant information and to enforce corrective action.	Both on site and pre-assessment	DO security	How are the individuals conducting the compliance audit review afforded the necessary authority to obtain relevant information and to enforce corrective action?		

Standard	Sect.	Section name	Sub-section	Requirement (standard language)	On site or pre-assessment	Question to:	Question	Response	
S58	8.1	Compliance audit programme and oversight	8.1.3	Compliance audit content 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.	Both on site and pre-assessment	DO security	Does the compliance audit review programme cover the entire mail security programme to ensure implementation of security requirements? Do the audits address facility security, personnel security, transportation and conveyance security?		
S58	8.1	Compliance audit programme and oversight	8.1.4	Compliance audit objectivity The DO shall ensure that the management of the compliance audit review programme shall be independent from individuals responsible for the implementation of the security requirements.	Both on site and pre-assessment	DO security	How do you ensure that the compliance audit review programme remains independent from those responsible for the implementation of the security requirements?		
S58	8.1	Compliance audit programme and oversight	8.1.5	Compliance audit results 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.	Both on site and pre-assessment	DO security	How are results of the compliance audits reported to the executive management of the DO?		
S58	9.1	Postal security unit for prevention and investigative management	9.1.1	Documented postal security programme 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. *EXAMPLE: Equipment, vehicles, uniforms, information technology, etc.*	Both on site and pre-assessment	DO security	Does the DO have a documented security programme covering the areas of prevention and investigation for the protection of mail, employees, partners, customers and postal assets? If so, please be prepared to share the documentation for review.		
S58	9.1	Postal security unit for prevention and investigative management	9.1.2	Postal security unit personnel The DO shall have a dedicated postal security unit or dedicated personnel to perform safety and security measures. The staff members dedicated to these functions shall be commensurate with the size and operations of the DO.	Both on site and pre-assessment	DO security	Does the DO have a dedicated postal security unit or dedicated personnel to perform safety and security measures? How many staff members are included in the unit or are responsible for performing safety and security? Do you have enough personnel dedicated to security functions? If not, what is not being done as a result of not having enough staff?		
S58	9.1	Postal security unit for prevention and investigative management	9.1.3	The dedicated postal security unit or dedicated security personnel shall perform periodic facility and process security reviews.	Both on site and pre-assessment	DO security	Does the dedicated postal security unit or dedicated security personnel perform periodic facility and process security reviews? Please be prepared to provide documentation of these reviews.		

Standard	Sect.	Section name	Sub-section	Requirement (standard language)	On site or pre-assessment	Question to:	Question	Response	
S58	9.2	Disaster recovery, emergency preparedness, and business continuity planning	9.2.1	Documented crisis plan The DO shall document and communicate to the 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.	Both on site and pre-assessment	DO security	Does the DO document and communicate to the 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. If yes, please be prepared to provide a copy of the plan.		
S58	9.2	Disaster recovery, emergency preparedness, and business continuity planning	9.2.2	Documented business continuity plan The DO shall document and communicate to the appropriate employees a business continuity plan to minimize postal interruption in the event of significant incident which might impact domestic or international postal operations.	Both on site and pre-assessment	DO security	Does the DO document and communicate to the appropriate employees a business continuity plan to minimize postal interruption in the event of significant incident which might impact domestic or international postal operations? If yes, please be prepared to provide a copy of the plan.		
S59	5.1	Custody of international airmail	5.1.1	Control custody of international airmail The DO shall maintain direct custody (by DO or designee) and control of international mail intended for conveyance by air from the time of acceptance until dispatched to the carrier/agent/designee. When a DO arranges to have a contractor or other entity accept international airmail on its behalf, the DO remains responsible for acceptance and handling of the mail. As such, the DO shall have processes in place whereby the contractor or other entity complies with these standards.	Both on site and pre-assessment	DO security	Please describe the custody procedures for international mail intended for carriage by air. Are these procedures also followed by contractors?		
S59	5.2	Items exempt from screening	5.2.1	Define exempted items When dispatching mail consisting of international postal items up to 500 grammes, the DO may dispatch it without additional screening if the DO has adhered to the security measures outlined in UPU S58. *Note: There may be other applicable international and/or national regulations which may define different thresholds for exemptions. Any exemptions applied should be in agreement with the appropriate national legislation or regulation. UPU member countries may agree to permit exemptions from screening or the use of alternative security measures because of the special nature of some types of mail. Such exemptions should be clearly defined in UPU member countries' National Civil Aviation Security Programme (NCASP).*	Both on site and pre-assessment	DO security	If mail pieces are exempted from screening, have they been agreed upon with national authorities? **Owing to security considerations and confidentiality, it may not be appropriate to list exempted items in this report.** How are the items that are exempted from screening kept separate from items that are subject to screening?		

Standard	Sect.	Section name	Sub-section	Requirement (standard language)	On site or pre-assessment	Question to:	Question	Response	
S59	5.3	Items to be screened	5.3.2	Screen mail items The DO or designee shall screen items by at least one of the following methods in accordance with the requirements of their national aviation security programme. As a minimum, the NCASP should reflect the standards and recommended practices set forth in ICAO Annex 17 and the guidance material in ICAO Aviation Security Manual, Doc 8973. –EDD; – EDS; – ETVD; – Manual search; – Metal detection; – X-ray equipment or other wave based systems.	Both on site and pre-assessment	DO security	Which mail screening standards are used? ICAO Annex 17 and the ICAO Aviation Security Manual, DOC 8973? **Owing to security considerations and confidentiality, it may not be appropriate to list screening standards in this report.**		
S59	5.4	High risk items	5.4.1	Define high-risk mail items Mail that requires additional security measures beyond baseline procedures is considered high risk. Mail or mail items can be considered high risk if there are: – anomalies in its nature that give rise to suspicion such as evidence of tampering; – due to its nature, baseline security measures alone are unlikely to detect prohibited articles as defined in the UPU postal security standards; – specific intelligence or threat information about it; – reasons to suspect that it contains or poses a threat based on risk assessment by an appropriate authority for aviation security, aircraft operators or other actors in the supply chain.	Both on site and pre-assessment	DO security	What is your definition for a high-risk mail item? Is that definition documented? Please be prepared to provide this documentation.		
S59	5.4	High risk items	5.4.2	Screen high-risk mail items The DO or designee shall screen high-risk items by viewing the item or receptacle from two angles and complying with national legislation OR – utilizing a combination of two or more screening methods below: – manual search ; – X-ray equipment; – EDD; – ETD.	Both on site and pre-assessment	DO security	Which screening methods are used to screen high-risk mail items (pieces or receptacles)? **Owing to security considerations and confidentiality, it may not be appropriate to list screening methods in this report.**		

Standard	Sect.	Section name	Sub-section	Requirement (standard language)	On site or pre-assessment	Question to:	Question	Response	
S59	5.5	Screening procedures for mail receptacles/bags	5.5.1	Screen mail receptacles/bags When authorized by their respective national authorities, the DO or designee shall utilize the technologies below to screen items already contained in receptacles/bags: – X-ray screening technology that is the most appropriate for the particular item or receptacle: i. the DO shall X-ray one receptacle at a time to search for indications of unauthorized explosives, incendiaries, and other destructive substances or items. ii. mail receptacles containing commodities that are too dense to render an accurate X-ray image shall be screened twice in succession, rotating the receptacle 90 degrees horizontally in either direction prior to screening it the second time, iii. if the X-ray image is unclear, shielded, or opaque or contains any unidentifiable anomalies, the DO shall clear the X-ray image by removing each mail piece from the receptacle and re-screen the individual pieces. and/or – EDD; and/or – EDS.	Both on site and pre-assessment	DO security	Describe your screening process in detail for items already contained in mail receptacles or bags. Which technologies are being used? **Owing to security considerations and confidentiality, it may not be appropriate to list which technologies are being used in this report.**		
S59	5.6	Alarm resolution of suspicious items	5.6.1	Clear suspicious items If the DO or screening designee identifies an item which cannot be cleared (alarm) during the initial screening, the item shall not be handed over to a carrier until the item is determined to be "Safe to fly": The item should be handled as a high risk item in accordance with Section 5.4 of these standards.	Both on site and pre-assessment	DO security	Please describe what happens when an item fails the initial screening. • What procedures do you follow to determine whether an item that fails initial screening is safe to fly? (Compare responses to standard)		
S59	5.7	Notification procedures	5.7.1	Isolation of failed mail pieces Cognizant of NCASP requirements, if the DO or screening designee cannot clear an item after following the procedures outlined above the mail item shall not be handed over, loaded or transported to any carrier/aircraft. The item shall be isolated in a secure location, controlled, and physically guarded to prevent unauthorized access to it.	Both on site and pre-assessment	DO security	When a suspicious mail item or receptacle cannot be resolved, what procedures are followed? What are the isolation and handling procedures for the suspicious mail item or receptacle?		

Standard	Sect.	Section name	Sub-section	Requirement (standard language)	On site or pre-assessment	Question to:	Question	Response	
S59	5.7	Notification procedures	5.7.2	Notification for failed mail pieces The DO or screening designee shall: – immediately contact the ground security coordinator, host government authorities, police, fire department, and/or bomb squad, according to local requirements; – inform entities identified of any additional international mail on the premises that was tendered or transferred with the suspect mail item.	Both on site and pre-assessment	DO security	When a suspicious mail item or receptacle cannot be resolved, what procedures are followed? What are the notification procedures? Do you notify: - the ground security coordinator; - host government authorities; - police; - fire department, and/or - bomb squad? Do you inform entities of any additional international mail on the premises that was tendered or transferred with the suspect mail item?		
S59	6.1	Measures for mail accepted/inducted for carriage on commercial aircraft	6.1.1	Mail security procedures The DO shall tender items to carriers, ground handling agents or other contractors for transport on aircraft in identifiable bags (receptacles) or containers affixed with the appropriate UPU forms or receptacle labels. After screening or the application of other security controls, mail shall be accounted for and protected from unauthorized interference prior to loading on an aircraft or secure exchange with the carrier, ground handling agent or other contractor. In accordance with their NCASP, a DO who has applied screening and security controls may be required to provide a consignment security declaration to the aircraft operator. The NCASP may also require additional record keeping for the purposes of an audit trail that the DO may need to address.	Both on site and pre-assessment	DO operations	After security controls have been applied, how is mail accounted for and protected from unauthorized interference prior to loading on an aircraft or secure exchange with the carrier?		