

- 4) Upon receipt of the property, the Receiving PC/LPC signs the G-504 and returns the original to the Transferring PC/LPC.
- 5) The Receiving PC/LPC scans and uploads the G-504 into Sunflower.
- 6) The Excess Clerk PC at the transferring office performs an “Excess Redeploy” transaction in Sunflower to change the asset’s status from “Excess” to “In Service” and initiates a transfer in Sunflower
 - The Excess Redeploy generates a request to the Receiving PC to accept the transfer in his/her steward code.
- 7) The Receiving PC/LPC accepts the transfer in Sunflower and verifies the steward code, location and asset user is correct.
- 8) The Receiving PC/LPC maintains a copy of the signed G-504 and any other supporting documentation for no less than three years after asset has been disposed of or transferred.

11.4.2 Excess Property Needed Within DHS

- 1) The interested DHS component contacts the ICE PC/LPC in possession of the excess property to request the asset.
- 2) The ICE PC/LPC prepares a DHS Form 560-3 for the receiving DHS component PC/LPC to sign.
- 3) For IT assets with data storage capability, the ICE PC/LPC confirms OCIO approval of the SF-120 and coordinates with the OCIO to ensure that the asset is sanitized before shipping.
 - a. The ICE PC/LPC completes a G-574 to temporarily transfer custody of the asset to the OCIO for sanitizing.
 - b. OCIO sanitizes the asset and returns it to the ICE PC/LPC along with a Certificate of HD Clean.
 - c. The ICE PC/LPC scans and uploads the Certificate of HD Clean into Sunflower.
- 4) The ICE PC/LPC sends the DHS Form 560-3 to the receiving DHS component PC/LPC along with the asset.
 - a. The receiving DHS component pays any costs associated with transferring the asset, including any shipping and/or handling fees.
- 5) Upon receipt of the property, the DHS component PC/LPC or APO signs the 560-3 and keeps a copy for their records. The signed original is returned to the ICE PC/LPC.

- 6) The ICE PC/LPC scans and uploads the 560-3 and any other supporting documentation into Sunflower.
- 7) The ICE PC/LPC final events the record as a “Transfer to Another Agency Within DHS.”
- 8) The ICE PC/LPC maintains the signed 560-3 and any other supporting documentation for no less than three years after asset has been disposed of or transferred.

11.5 External Screening (21 Days)

- 1) If the asset is not claimed by the end of the 21 day internal screening within ICE and DHS, it is reported to GSA. This reporting occurs through an automatic batch upload into GSAXcess® via the Sunflower/GSAXcess® interoperability function for all assets that are recorded in Sunflower. All other assets must be manually entered into GSAXcess®.
- 2) Excess property successfully processed through the batch upload receives an ‘Item Control Number’ in GSAXcess®. The Item Control Number links property records in GSAXcess® to those in Sunflower and is included along with the date of the upload in the ‘GSA Excess Information’ field of the ‘Maintain Excess Assets’ screen in the Sunflower Excess Module. A blank GSA Excess Information field indicates the property record has not been batch uploaded into GSAXcess®
- 3) Item Control Numbers for all ICE property that is automatically uploaded into GSAXcess® will begin with the ICE Activity Address Code (AAC) of 7031AA, regardless of the ICE Program Office or location that owns the asset. The AAC is a six digit alpha-numeric code assigned to identify specific units, activities, or organizations that have procurement authority and authority to requisition and receive excess or surplus property.
- 4) The batch upload will not include excess property that has not been designated as “Excess” in Sunflower or has been transferred and/or final evented before the end of the 21 day internal screening period.
- 5) Accountable personal property that is not recorded in Sunflower must be manually entered into GSAXcess® with the AAC code 7031AA.

11.5.1 Computers for Learning Program

Computers for Learning (CFL) is a program that allows Federal agencies to provide computers to educational organizations in accordance with Executive Order 12999, which directs Federal agencies to give “highest preference to schools and nonprofits in the transfer of educationally useful federal equipment.” An educational nonprofit entity is eligible for CFL computers if it meets all of the following criteria:

- Is tax exempt under section 501 (c) of the U.S. tax code.

- Serves some portion of the pre-kindergarten through grade 12 population.
- Operates exclusively for the purpose of education.
- Submits the request on the school's letterhead.

Schools and/or educational non-profit organizations that wish to receive these computers must register with the CFL program via the CFL website (www.computers.fed.gov).

11.5.2 Pre-selected CFL Recipient

If the Program Office identifies a CFL program participant to receive the asset, before or during the course of the internal screening process, the PC/LPC should work expeditiously to transfer the asset directly to the CFL participant before the asset is automatically uploaded into GSAXcess® at the end of the 21 day internal screening period.

Note: If an ICE office has already identified a CFL participant to whom it wants to transfer the asset, but was unable to complete the transfer before the asset was batch uploaded to GSAXcess®, it can remove the asset from participating in CFL screening.

- a. The ICE PC/LPC instructs the pre-selected CFL participant to request the asset via the CFL program website.
 - b. The CFL program notifies GSAXcess® of the request electronically.
 - c. GSAXcess® forwards the pre-selected CFL participant's request via email to the ICE PC/LPC for processing (please refer to steps 1 through 11 in Section 11.5.3).
- 1) The ICE PC/LPC prepares an SF-122 (see Appendix C Forms) and Certificate of Disposal for the CFL recipient to sign.
 - a. Both an ICE official and an authorized school official (Principal, Vice Principal, Administrator, etc.) must complete and sign the Certificate of Disposal.
 - 2) The ICE PC/LPC confirms OCIO approval of the SF-120 and coordinates with the OCIO to ensure that the asset is sanitized before shipping.
 - a. The ICE PC/LPC completes a G-574 to indicate that OCIO has temporary custody of the asset for sanitizing.
 - b. OCIO sanitizes the asset and returns it to the ICE PC/LPC along with a Certificate of HD Clean.
 - c. The ICE PC/LPC scans and uploads the Certificate of HD Clean into Sunflower.
 - 3) The ICE PC/LPC removes and stores the ICE barcode label with the property documentation.
 - a. If the barcode is destroyed during removal, the ICE PC/LPC must make sure the full barcode has been removed from the asset, and must mark the barcode number and the form of destruction in the asset Sunflower record and/or documentation folder.

- 4) The ICE PC/LPC signs the Certificate of Disposal with two witnesses present.
- 5) The ICE PC/LPC sends the SF-122 and Certificate of Disposal to the CFL recipient along with the asset.
 - a. The CFL recipient pays any costs associated with transferring the asset, including any shipping and/or handling fees.
- 6) The CFL recipient signs and returns the original SF-122 and Certificate of Disposal to the ICE PC/LPC.
- 7) The ICE PC/LPC scans and uploads the SF-122, Certificate of Disposal, and any other supporting documentation into Sunflower.
- 8) The ICE PC/LPC final events the record to “Donation to a School/Non-Profit Educational Inst.” The school’s registration code, which can be obtained from the NUO, must also be included.
- 9) The ICE PC/LPC maintains the SF-122, Certificate of Disposal, and any other supporting documentation for no less than three years after the transfer of the asset.
 - Supporting documents for excess property screened externally include:
 - Transfer Order (e.g., SF-122)
 - Certificate of Disposal
 - Shipping documentation
 - Barcode label (retained in hardcopy)

11.5.3 Non Pre-selected CFL Recipient

CFL eligible assets not selected and/or final evented at the end of the 21 day internal screening process will be batch uploaded into GSAXcess® and made available exclusively for selection by CFL program participants for the first 7 days out of the 21 day internal screening period.

GSAXcess® automatically designates CFL eligible assets for participation in CFL screening based on the asset’s Federal Supply Code (FSC). The Item control number is used for reference and is posted in Sunflower when batch upload is complete.

If a CFL participant requests the excess property via the CFL program website, the CFL program will notify GSAXcess® of the request electronically. GSAXcess® will forward an allocation request via email to the designated ICE PC/LPC for processing.

- 1) The ICE PC/LPC logs into the GSAXcess® ‘View/Allocate Requested Item’ screen and approves the request to allocate the property to the CFL participant.

- 2) Upon the ICE PC/LPC's approval of the allocation request, GSAXcess® generates a SF-122 and sends it electronically to the ICE PC/LPC, designated ICE HQ Approving Official, and CFL recipient for approval.
- 3) The ICE PC/LPC prepares a Certificate of Disposal for the CFL recipient to sign.
 - Both an ICE official and an authorized school/educational non-profit official (Principal, Vice Principal, Administrator, etc.) must complete and sign the Certificate of Disposal.
- 4) Once the ICE PC/LPC and ICE HQ Approving Official have signed the SF-122, the ICE PC/LPC confirms OCIO approval of the SF-120 and coordinates with the OCIO to ensure that the asset is sanitized before shipping.
 - a. The ICE PC/LPC completes a G-574 to indicate that OCIO has temporary custody of the asset for sanitizing.
 - b. OCIO sanitizes the asset and returns it to the ICE PC/LPC along with a Certificate of HD Clean.
 - c. The ICE PC/LPC scans and uploads the Certificate of HD Clean into Sunflower.
- 5) The ICE PC/LPC removes and stores the ICE barcode label with the property documentation.
 - a. If the barcode is destroyed during removal, the ICE PC/LPC must make sure the full barcode has been removed from the asset, and must mark the barcode number and the form of destruction in the asset Sunflower record and/or documentation folder.
- 6) The ICE PC/LPC signs the Certificate of Disposal with two witnesses present.
- 7) The ICE PC/LPC sends the Certificate of Disposal to the CFL recipient along with the asset.
 - a. The CFL recipient pays any costs associated with transferring the asset, including any shipping and/or handling fees.
- 8) The CFL recipient signs and returns the original SF-122 and Certificate of Disposal to the ICE PC/LPC.
- 9) The ICE PC/LPC scans and uploads the SF-122, Certificate of Disposal, and any other supporting documentation into Sunflower.
- 10) The ICE PC/LPC final events the record to "Donation to a School/Non-Profit Educational Inst." The school's registration code, which can be obtained from the ICE NUO, must also be included.

- 11) The ICE PC/LPC retains the fully executed SF-122, Certificate of Disposal, and any other supporting documentation for no less than three years after the transfer of the asset.

11.5.4 Excess Property Re-Utilized by Other Federal Agencies

Excess assets that are not selected during internal screening or for participation in the CFL Program are made available for re-utilization by other Federal agencies for 21 days. Excess property that is screened for CFL Program use, but not selected by the end of the 7-day CFL Program screening period in GSAXcess, is eligible for re-utilization by other Federal agencies; however, the screening period is limited to 14 days as the 7-day CFL Program screening period counts towards the 21-day external screening process.

If an asset is requested by a federal agency outside DHS, GSA coordinates the transfer of the asset. The other federal agency may be required to reimburse ICE for the fair value of the property. The fair value is determined by ICE (see Chapter 7 Acquisition Costs and Values).

- 1) Upon approving the allocation of excess property, GSAXcess® generates an electronic notification to the requesting agency's Approving Official to advise that electronic approval of an SF-122 is required for excess property selected by another Federal agency.
- 2) Once the requesting agency's Approving Official approves the SF-122 electronically, GSA signs the SF-122, requisitions the property in GSAXcess®, and sends a copy of the fully executed SF-122 to both the ICE PC/LPC and the requesting agency.
- 3) The requesting Federal agency coordinates the transfer of the asset with the ICE PC/LPC.
- 4) The ICE PC/LPC prepares a Certificate of Disposal for the receiving agency to sign.
- 5) For IT assets with data storage capability, the ICE PC/LPC confirms OCIO approval of the SF-120 and coordinates with the OCIO to ensure that the asset is sanitized before shipping.
 - a. The ICE PC/LPC completes a G-574 to temporarily transfer custody of the asset to the OCIO for sanitizing.
 - b. OCIO sanitizes the asset and returns it to the ICE PC/LPC along with a Certificate of HD Clean.
 - c. The ICE PC/LPC scans and uploads the Certificate of HD Clean into Sunflower.
- 6) The ICE PC/LPC removes and stores the ICE barcode label with the property documentation.
 - a. If the barcode is destroyed during removal, the ICE PC/LPC must make sure the full barcode has been removed from the asset, and must mark the barcode number and the incidence of destruction in the asset Sunflower record and/or documentation folder.

- 7) The ICE PC/LPC signs the Certificate of Disposal with two witnesses present.
- 8) The ICE PC/LPC sends the Certificate of Disposal to the receiving agency along with the asset.
 - The receiving agency pays any costs associated with transferring the asset, including any shipping and/or handling fees.
- 9) The receiving agency signs and returns the original Certificate of Disposal to the ICE PC/LPC.
- 10) The ICE PC/LPC scans and uploads the SF-122, Certificate of Disposal, and any other supporting documentation into Sunflower.
- 11) The ICE PC/LPC final events the Sunflower record to “Transfer of Excess to Another Federal Agency – SF-122.”
- 12) The ICE PC/LPC maintains the SF-122, Certificate of Disposal, barcode labels, and any other supporting documentation for no less than three years after the transfer of the asset.

11.6 Donating Property

If an excess asset has not been re-utilized by the completion of the 21 day external screening process, the asset becomes surplus property and is made available for donation to non-Federal entities that requested it during external excess screening for five days via GSAXcess®. An asset must be donated to a non-Federal entity in compliance with 41 CFR 102-37. The major categories of eligible recipients are:

- Public agencies
 - Non-profit educational and public health activities
 - Non-profit and public programs for the elderly
 - Public airports
 - Providers of assistance to the homeless
- 1) Upon approving the allocation of surplus property, GSAXcess® generates an electronic notification to the requesting non-Federal entity’s Approving Official to advise that electronic approval of an SF-123 Transfer Order Surplus Personal Property (see Appendix C Forms) is required for property they selected during the external excess screening process.
 - 2) Once the requesting non-Federal entity’s Approving Official approves the SF-123 electronically, GSA signs the SF-123, requisitions the property in GSAXcess®, and sends a copy of the fully executed SF-123 to both the ICE PC/LPC and the requesting non-Federal entity.

- 3) The requesting non-Federal entity coordinates the transfer of the asset with the ICE PC/LPC.
- 4) The ICE PC/LPC prepares a Certificate of Disposal for the requesting non-Federal entity to sign.
- 5) For IT assets with data storage capability, the ICE PC/LPC confirms OCIO approval of the SF-120 and coordinates with the OCIO to ensure that the asset is sanitized before shipping.
 - a. The ICE PC/LPC completes a G-574 to temporarily transfer custody of the asset to the OCIO for sanitizing.
 - b. OCIO sanitizes the asset and returns it to the ICE PC/LPC along with a Certificate of HD Clean.
 - c. The ICE PC/LPC scans and uploads the Certificate of HD Clean into Sunflower.
- 6) The ICE PC/LPC removes the ICE barcode label and stores it with the property documentation.
 - a. If the barcode is destroyed during removal, the PC/LPC must make sure the full barcode has been removed from the asset, and must mark the barcode number and the form of destruction in the asset Sunflower record and/or documentation folder.
- 7) The ICE PC/LPC signs the Certificate of Disposal with two witnesses present.
- 8) The ICE PC/LPC sends the Certificate of Disposal to the requesting non-Federal entity along with the asset.
 - a. The receiving entity pays any costs associated with transferring the asset, including any shipping and/or handling fees.
- 9) The receiving non-Federal entity signs and returns the original Certificate of Disposal.
- 10) The Transferring PC/LPC scans and uploads the SF-123, Certificate of Disposal, and any other supporting documentation into Sunflower.
- 11) The Transferring PC/LPC creates a final event record in Sunflower as "Donation to other Non-Federal Recipients."
- 12) The ICE PC/LPC maintains the signed SF-123, Certificate of Disposal, barcode labels, and any other supporting documentation for no less than three years after the transfer of the asset.

11.7 Disposing of Property through Sales

If an excess asset has not been re-utilized or donated, then it may be made available for sale to

the public via GSA as authorized by the approved SF-120. GSA offers several options to sell property for a fee, and will determine which method is most appropriate. Avenues for selling property through GSA include:

- GSA Auctions®
- Live auction
- Fixed price
- Drop-by
- Negotiated
- Sealed bid

ICE can also elect to manage the sale of property itself by obtaining an approved waiver from GSA and working with an approved Contracting Officer to conduct the sale. Details on obtaining a waiver are available by emailing the Federal Asset Sales Central Planning Office at

(b) (7)(E) @gsa.gov.

11.7.1 GSA Auctions®

The GSA Auctions® (www.gsaauctions.gov) offers the general public the opportunity to bid electronically on a wide array of Federal assets. The auctions are completely web-enabled, allowing all registered participants to bid on a single item or multiple items (lots) within specified timeframes.

Unless specified otherwise, GSAXcess® will automatically transfer records for property that cannot be re-utilized or donated to GSA Auctions® for sale.

11.7.2 MySales

MySales allows Federal agencies to monitor the status of their surplus and exchange/sale property that has transitioned into the GSA Sales Program. By using MySales, agencies will have the ability to report, modify, and maintain information on their property for sale.

To access MySales:

- 1) Obtain an application from GSA at <http://mysales.fss.gsa.gov/sasy/sasywel>
- 2) Submit the application to the ICE NUO, on the [located](#) POC section of the Property Branch intranet page at <http://intranet.ice.dhs.gov/cfo/sites/OAA/pmb/poc.htm>

11.7.3 Sales Process

For sales through GSA, specific processes must be followed to prepare the asset for sale and complete the transaction in accordance with the regulations under 41 CFR 102-38.

- 1) Once an asset is purchased, the purchaser coordinates the transfer of the asset with the ICE PC/LPC.

- 2) The ICE PC/LPC prepares a Certificate of Disposal for the purchaser to sign.
- 3) For IT assets with data storage capability, the ICE PC/LPC confirms OCIO approval of the SF-120 and coordinates with the OCIO to ensure that the asset is sanitized before shipping.
 - The ICE PC/LPC completes a G-574 to temporarily transfer custody of the asset to the OCIO for sanitizing.
 - OCIO sanitizes the asset and returns it to the ICE PC/LPC along with a Certificate of HD Clean.
 - The ICE PC/LPC scans and uploads the Certificate of HD Clean into Sunflower.
- 4) The ICE PC/LPC removes and stores the ICE barcode label with the property documentation.
 - If the barcode is destroyed during removal, the PC/LPC must make sure the full barcode has been removed from the asset, and must mark the barcode number and the form of destruction in the asset Sunflower record and/or documentation folder.
- 5) The ICE PC/LPC signs the Certificate of Disposal with two witnesses present.
- 6) The ICE PC/LPC sends the Certificate of Disposal to the purchaser along with the asset.
 - a. The purchaser pays any costs associated with transferring the asset, including any shipping and/or handling fees.
- 7) The purchaser signs and returns the original Certificate of Disposal to the ICE PC/LPC.
- 8) The ICE PC/LPC scans and uploads the signed Certificate of Disposal and any other supporting documentation into Sunflower.
- 9) The ICE PC/LPC creates a final event record in the Sunflower Excess Module for “Exchange, Sale or Trade-in” as applicable.
- 10) The ICE PC/LPC maintains the signed Certificate of Disposal and any other supporting documentation for no less than three years after the transfer of the asset.

11.7.4 Exchange/Sale of Property

When acquiring replacement property, Federal agencies may exchange or sell similar items and may apply the exchange allowance or proceeds of sale in whole or in part payment for the property acquired. Disposal of property through exchange/sale occurs outside of the excess screening and disposal process. The exchange/sale process must be completed in accordance with the regulations under 41 CFR 102-39.

- 1) The ICE PC/LPC completes a SF-126 Report of Personal Property for Sale form (see Appendix C Forms) and sends the original to GSA to report the exchange/sale property for sale.
- 2) The ICE PC/LPC maintains a copy of the SF-126 with the property documentation.
- 3) GSA determines the appropriate sales method and makes the asset available for sale.
- 4) Once the asset is purchased, the purchaser coordinates the transfer of the asset with the ICE PC/LPC.
- 5) For IT assets with data storage capability, the ICE PC/LPC confirms OCIO approval of the SF-120 and coordinates with the OCIO to ensure that the asset is sanitized before sending.
 - a. The ICE PC/LPC completes a G-574 to temporarily transfer custody of the asset to the OCIO for sanitizing.
 - b. OCIO sanitizes the asset and returns it to the ICE PC/LPC along with a Certificate of HD Clean.
 - c. The ICE PC/LPC scans and uploads the Certificate of HD Clean into Sunflower.
- 6) The ICE PC/LPC removes and stores the ICE barcode label with the property documentation.
 - a. If the barcode is destroyed during removal, the ICE PC/LPC must make sure the full barcode has been removed from the asset, and must mark the barcode number and the form of destruction in the asset Sunflower record and/or documentation folder.
- 7) The ICE PC/LPC signs the Certificate of Disposal with two witnesses present.
- 8) The ICE PC/LPC delivers the asset to the purchaser along with the Certificate of Disposal.
- 9) The purchaser signs and returns the original Certificate of Disposal or an authorized GSA Bill of Sale to the ICE PC/LPC.
- 10) The ICE PC/LPC scans and uploads the signed SF-126, Certificate of Disposal, and any other supporting documentation into Sunflower.
- 11) The ICE PC/LPC final events the record in the Sunflower Management module as "Exchange/Sale." The PC must also provide to the sales proceeds.
- 12) The ICE PC/LPC maintains the signed Certificate of Disposal and any other supporting documentation for no less than three years after the transfer of the asset.

11.7.5 Sales Proceeds

Sales proceeds are the funds that are returned to ICE on the sale of personal property. Net sales proceeds (sales proceeds less GSA's direct and indirect costs) that are reimbursable to ICE must be distributed to ICE via the On-line Payment and Accounting Control System (OPAC).

GSA retains a portion of the proceeds from the sale of non-reimbursable surplus property. The net proceeds will be deposited to miscellaneous receipts of the Treasury.

11.8 Abandonment or Destruction

If an asset has not been re-utilized, donated, or sold, it may be abandoned or destroyed in some circumstances. In many cases, disposal by abandonment or destruction is strictly mandated by law, regulation, or ICE directive for reasons of public health, safety, or security. No property should be abandoned or destroyed without thoroughly researching these requirements regardless of whether they are identified in this handbook or not. Written approval from GSA or NUO is required before property can be abandoned or destroyed.

Abandonment is discouraged except in the rare instances when it is deemed most beneficial to the Government by following the procedures below.

Note: Personal effects of defendants or detainees are not to be considered "personal property" for the purposes of the Personal Property Management Policy or the Personal Property Operations Handbook."

- 1) Upon receipt of written GSA disposal approval, the ICE PC/LPC identifies the proper authority or justification for the disposal. These authorities are:
 - a. The property has no commercial value. No commercial value means that the property, through determination, has neither utility nor monetary value (either as an item or as scrap).
 - b. The cost of care, handling, and preparation of the property for sale would be greater than the expected sale proceeds (estimated fair value).
 - c. A law, regulation, or directive requires abandonment or destruction.
 - d. Written instructions by a duly authorized official (*e.g.*, health and safety officer or security officer) directing abandonment or destruction.
- 2) Abandonment or destruction of ICE surplus property must be documented properly and must meet all audit trail requirements (*i.e.* all supporting documentation from acquisition to disposal must be present, and for a period of 3 years after the disposal takes place). Great care must be taken to fully justify and document all actions related to abandonment or destruction.
- 3) Upon delegated authority from the ICE APO, the ICE PC/LPC prepares a written finding justifying the abandonment or destruction action (for additional detail see 41 CFR 102-36). The written finding includes:

- a. A detailed description of the property including the property control number, serial number, condition, and total acquisition cost.
 - b. The authority for the abandonment or destruction action along with any pertinent supporting documentation.
 - c. A statement describing the proposed method of destruction (i.e., burning, burying) or the abandonment location with guidance from a duly authorized official on how to dispose of the asset safely.
 - d. A statement from the duly authorized official that the proposed abandonment or destruction action is not detrimental or dangerous to public health or safety and will not infringe on the rights of other persons.
 - e. The signature of the ICE PC/LPC approving the abandonment or destruction of property with an acquisition cost below \$1,000. The ICE APO's signature is required for personal property with an acquisition cost of over \$1,000.
- 4) The ICE PC/LPC provides public notice of the abandonment or destruction action for a period not less than seven calendar days. Any exceptions to this notice must comply with the 41 CFR 102-36. The public can be notified by posting announcements in public places or publishing the announcement in organizational newsletters and must include:
- General description of the property
 - Date and location of the abandonment or destruction action

11.8.1 Abandonment

- 1) The ICE PC/LPC prepares and forwards the written justification and Certificate of Disposal to ICE APO for approval.
- 2) The ICE APO indicates that the asset is to be abandoned in accordance with the instructions provided by the duly authorized official in the written justification and returns the Certificate of Disposal to the ICE PC/LPC.
- 3) For IT assets with data storage capability, the ICE PC/LPC confirms OCIO approval of the SF-120 and coordinates with the OCIO to ensure that the asset is sanitized before shipping.
 - a. The ICE PC/LPC completes a G-574 to temporarily transfer custody of the asset to the OCIO for sanitizing.
 - b. OCIO sanitizes the asset and returns it to the ICE PC/LPC along with a Certificate of HD Clean.
 - c. The ICE PC/LPC scans and uploads the Certificate of HD Clean into Sunflower.
 - d. The PC/LPC submits the signed SF-120 to the ICE NUO through his or her HPPM.
- 4) The ICE PC/LPC removes and stores the ICE barcode label with the property documentation.

- a. If the barcode is destroyed during removal, the ICE PC/LPC must make sure the full barcode has been removed from the asset, and must mark the barcode number and the form of destruction in the asset Sunflower record and/or documentation folder.
- 5) The ICE PC/LPC signs the Certificate of Disposal with two witnesses present.
- 6) The ICE PC/LPC abandons the asset in its existing location.
- 7) The ICE PC/LPC scans and uploads the Certificate of Disposal and any other supporting documentation into Sunflower.
- 8) The ICE PC/LPC Final Events the record in Sunflower as “Abandoned” when applicable.
- 9) The ICE PC/LPC maintains the signed Certificate of Disposal and any other supporting documentation for no less than three years after the abandonment of the asset.

11.8.2 Destruction

- 1) The ICE PC/LPC prepares and forwards the written justification and Certificate of Disposal to the ICE APO for approval.
- 2) The ICE APO approves the Certificate of Disposal and indicates that the asset is to be destroyed in accordance with the instructions provided by the duly authorized official in the written justification.
- 3) For IT assets with data storage capability, the ICE PC/LPC confirms OCIO approval of the SF-120 and coordinates with the OCIO to ensure that the asset is sanitized before shipping.
 - a. The ICE PC/LPC completes a G-574 to temporarily transfer custody of the asset to the OCIO for sanitizing.
 - b. OCIO sanitizes the asset and returns it to the ICE PC/LPC along with a Certificate of HD Clean.
 - c. The ICE PC/LPC scans and uploads the Certificate of HD Clean into Sunflower.
 - d. The PC/LPC submits the signed SF-120 to the ICE NUO through his or her HPPM.
- 4) The ICE PC/LPC removes and stores the ICE barcode label with the property documentation.
 - a. If the barcode is destroyed during removal, the ICE PC/LPC must make sure the full barcode has been removed from the asset, and must mark the barcode number and the incidence of destruction in the asset Sunflower record and/or documentation folder.

- 5) The ICE PC/LPC signs the Certificate of Disposal with two witnesses present.
- 6) The ICE PC/LPC delivers the asset to the disposing entity along with the Certificate of Disposal; examples include UNICOR and eWaste.
- 7) The Disposing entity signs and returns the original Certificate of Disposal to the ICE PC/LPC.
- 8) The ICE PC/LPC scans and uploads the Certificate of Disposal and any other supporting documentation into Sunflower.
- 9) The ICE PC/LPC final events the record in Sunflower as “Recycled”.
 - The disposing agency generally recycles most property it receives. If, however, the PC/LPC knows with certainty that property will be destroyed, the Sunflower record should be final evented as “Destroyed”.
- 10) The ICE PC/LPC maintains the signed Certificate of Disposal and any other supporting documentation for no less than three years after the destruction of the asset.

Chapter 12

12. REPORTING REQUIREMENTS

OVERVIEW

ICE is required to complete and file asset related reports for various stakeholders. In addition to financial reports, GSA requires ICE to report annual property management activity in such areas as disposal, physical inventory, and donation through the CFL program. The DHS and ICE OAA also may require program offices to complete ad hoc reports.

PROCEDURES

12.1 Monthly Reports

- 1) Changes in capitalized asset status must be reported to OAA, for new incoming assets, as well as adjustments to existing asset records, and outgoing disposed assets. Changes to capital assets and their depreciation are reported by OAA to OFM on a monthly basis.
- 2) All ROS documentation must be submitted by all Programs to OAA for tracking and accountability purposes on a monthly basis. OAA follows assets from acquisition to disposal and needs the documentation on hand for audit purposes.

12.2 Annual Report of Lost, Damaged, or Destroyed Property

- 1) Within 60 calendar days after the close of every fiscal year, and on a quarterly basis, ICE submits a single consolidated Annual Report of Lost, Damaged, or Destroyed Property (LDD) in memorandum format to DHS. The report is compiled from the input of Headquarters, offices, and other organizations.
- 2) The PC/LPC submits the LDD report to their HPPMs on a monthly basis via email. The report is required monthly even if there has been no LDD to report (negative report). Negative reports contain information regarding assets that have been lost, damaged, or destroyed, as they will be counted as a loss against the property and possibly financial record.
- 3) PC/LPC follows all disposal guidance for assets that have been damaged (see Chapter 11, Disposal)
- 4) The HPPM submits the consolidated LDD report to the Property Branch. Negative reports are required.
 - a. Negative reports are reports that must be submitted stating that no LDD has occurred. Negative reports are required so the Property Branch has an official response on file from each Program Office.
- 5) The Property Branch submits the consolidated LDD report to DHS OAA. Negative reports are required.

Note: Specific reporting instructions will be distributed by OAA Property Branch on a yearly basis noting when the reports are due.

12.3 Government Property Furnished to Contractors

- 1) Within 90 calendar days after the beginning of the calendar year, each organizational element submits a single consolidated report for Government Property Furnished to Contractors (GFE). The report is compiled from the input of Headquarters, field offices, and other field organizations.
- 2) The APO requests that contractors complete a GFE to Contractors report, inventorying all the government assets in the contractor's possession.
- 3) The APO submits the GFE to Contractors report to HPPMs by March 1 of each fiscal year. Negative reports are required.
- 4) The HPPM submits the consolidated GFE Report to the Property Branch by March 15 of each fiscal year. Negative reports are required.
- 5) The Property Branch submits consolidated GFE Reports to DHS Office of Asset Administration by March 30 of each fiscal year. Negative reports are required.

12.4 Annual Inventory Plan

- 1) Within 30 days after the beginning of the calendar year, the Property Branch submits an Annual Inventory Plan to DHS OAA, outlining its plan for conducting an annual physical inventory.

12.5 Excess Property Furnished to Non-Federal Recipients

- 1) Within 60 calendar days after the close of each fiscal year, each executive agency must submit a single consolidated report of all personal property furnished to non-Federal recipients (donation). The report is compiled from the input of Headquarters, field offices, and other field organizations.
- 2) The APOs request all information regarding Excess Property Furnished to Non-Federal Recipients from relevant parties, inventorying all government property in the parties' possession.
- 3) The APOs submit the Excess Property Furnished to Non-Federal Recipients report to their HPPMs by October 15 of each fiscal year. Negative reports are required.
- 4) The HPPMs submit consolidated Excess Property Furnished to Non-Federal Recipients report to the Property Branch by November 1 of each fiscal year. Negative reports are required.
- 5) The Property Branch submits the consolidated Excess Property Furnished to Non-Federal Recipients report to DHS OAA, no later than November 30 of each fiscal year.

12.6 Exchange / Sale Transactions

- 1) The APO requests all information regarding any Exchange / Sale Transactions from relevant parties.
- 2) The APO submits the Exchange / Sale Transactions report to the HPPM by October 15 of each fiscal year. Negative reports are required.
- 3) The HPPMs submits the consolidated Exchange / Sale Transactions report to the Property Branch by November 1 of each fiscal year. Negative reports are required.
- 4) The Property Branch submits the consolidated Exchange / Sale Transactions report to DHS OAA no later than November 30 of each fiscal year. Negative reports are required.

12.7 Computers for Learning Donations

Except on very rare occasions, CFL donations are completed through the CFL website, <http://computersforlearning.gov/>. In the event that a CFL donation is not completed through the CFL website, the following process applies:

- 1) The APO requests all documentation from PCs involved with the CFL Donation program and compiles them into a single report.
- 2) The APO submits the CFL Donation report to the HPPM by November 1 of each fiscal year.
- 3) The HPPM submits the consolidated CFL Donation report to the Property Branch by November 15 of each fiscal year.
- 4) The Property Branch submits the consolidated CFL Donation report to DHS OAA no later than November 30 of each fiscal year.

Chapter 13

13. MONITORING AND OVERSIGHT FUNCTIONS

OVERVIEW

Quality review takes place at various points throughout the asset management lifecycle. Quality reviews verify that all property is managed in accordance with federal regulations, policies, and accountability standards. Reviews are conducted by the OAC ORG, Office of Financial Management (OFM), and OAA. The goal is to improve the accuracy, completeness, and value of Sunflower records and the resulting financial transactions.

PROCEDURES

13.1 Acquisition Reviews

- 1) ORG performs monthly quality reviews that balance monies spent against assets that are coming into the organization on a monthly basis, ensuring assets that have been purchased have been entered in Sunflower and that all source documentation is available and correct, etc. Several Sunflower entries include:
 - Open obligations vs. Sunflower records
 - Vehicle production reports vs. Sunflower additions
 - Sunflower capital asset records contain supporting documentation
 - Documentation supports asset value
- 2) OFM runs a monthly report of assets in Sunflower to identify capital assets and adjust FFMS accounts accordingly.

13.2 Inventory Reviews

- 1) The Property Branch performs quality assurance reviews of inventory results throughout the annual inventory process and provides feedback to Program Offices as needed.
- 2) The Property Branch performs an end-of-inventory quality control review.
- 3) The Property Branch reviews inventory data from selected sites to evaluate the success of the inventory and to identify lessons learned.
- 4) OFM reviews inventory results quarterly for newly added capitalized assets and adjusts FFMS to reflect correct depreciation of assets or other adjustments.
- 5) ORG and OAA review Sunflower records created during inventory to determine if assigned value is supportable.

- 6) ORG and OAA conduct periodic quality checks of inventory samples throughout the fiscal year and work with Program Offices to resolve discrepancies.

13.3 Excessing Reviews

- 1) The ICE NUO receives approved SF-120s (see Appendix C Forms) and maintains record of ICE property designated as excess for submission to ORG during monthly quality assurance reviews.

13.4 Disposal Reviews

- 1) ORG compares vehicle disposal reports vs. Sunflower retirements.
- 2) ORG compares GSA disposal reports vs. Sunflower retirements.
- 3) OFM runs monthly Sunflower reports to identify disposed accountable capital assets and adjusts property, plant, and equipment accounts in FFMS accordingly.

Glossary

A

Abandoned (or Unclaimed Property): Personal property that is found on premises owned or leased by ICE and is subject to the filing of a claim by the former owner within 3 years of vesting of title in the United States.

Accountability: The act of maintaining an account (record) for personal property by providing a complete audit trail for property transactions from receipt to final disposition.

Accountable Personal Property: The personal property with an initial acquisition cost at, or above, a specific threshold [\$5,000 at ICE], and items designated as sensitive, that must be controlled and recorded in the organization's automated control system. Accountable items may be either capitalized or non-capitalized.

Note: Regardless of whether property meets the definition of "accountable personal property", ICE organizations must develop and maintain internal controls that provide reasonable assurance that all property is managed in accordance with federal laws, regulations, and DHS and ICE policy.

Acquisition: To procure, purchase, or obtain personal property in accordance with Federal Acquisition Regulations (FAR) and ICE Management Directives, including, but not limited to transfer, donation, forfeiture, manufacture, or production at Government-owned plants or other facilities.

Acquisition Cost: The unit price of an item including all costs required to put the asset into its intended use.

Activity Address Code (AAC): The six-position alpha-numeric code assigned to identify specific units, activities, or organizations that have procurement authority and authority to requisition and receive excess or surplus property. The AAC is used to identify and bill requestors of excess property for shipping/handling costs.

Administratively Controlled Property: Property with an acquisition cost below \$5,000 that is not recorded as sensitive, which is subject to reasonable controls relative to property values. At a minimum, consumable property (supplies and spare parts) should have double entry accounting records as to what was received and to whom it was issued.

B

Barcode: A Personal Property Control Number (PCCN) used to identify Personal Property. It must comply with the design, specifications, and standards established and approved by OAA Property Branch.

Boards of Survey: Standing or ad hoc committees designated, as needed, to adjudicate Reports

of Survey. The Program Board of Survey adjudicates Reports of Survey referred from the APO to the Headquarters Program Property Manager. In the case of a National Board of Survey, Reports of Survey are referred from the Headquarters Program Property Manager to the OCFO/OAA/Property Management Branch.

C

Capital Leases: Transfer substantially all the benefits and risks of ownership to the lessee and transfers ownership of the property to the lessee by the end of the lease term or contains an option to purchase the leased property at a bargain price.

Capitalized Software: Software (COTS, internally developed software, or contractor developed software) that is \$750,000 or more of developmental phase cost. Prior to October 1, 2003, the capitalization threshold was \$500,000.

Capitalization: Financial management term that describes the function of recording the total acquisition cost of an item in the general ledger of ICE's financial accounts in order to accurately reflect the agency's investment in the asset. The recording of and carrying forward of an expense into one or more future periods, results in expensing the cost of an asset over the remainder of its useful life by matching the benefit gained from that expenditure with the associated cost.

Capitalized Personal Property: Property with an initial cost at or above the criteria established by the GAO in Title 2 of its "Policy and Procedures Manual for Guidance of Federal Agencies" which is recorded in the general ledger of the financial management accounts. An agency may select a lower capitalization level than that established by GAO. To identify what is to be captured as capitalized fixed asset, the OCFO/Office of Financial Management issues criteria for managers to go by. Capitalized personal property has an estimated service life of two years or more and is acquired at or above a specified cost established in DHS Management Directive 1120.1.

Condition Codes: Codes that consist of an alpha code (supply) and a numeric code (disposal) that describe the physical condition, readiness for issue, and serviceability of personal property.

Contractor Inventory: Personal property furnished to, or acquired by, and in the possession of a contractor pursuant to the terms of a contract, in which title is vested in the Government.

Custodial Area: A subdivision of an accountable area, defined by organizational or geographical limits, for which a property custodian has been designated. For ICE a custodial area is represented by the steward code or set of steward codes for which an individual is the property custodian.

D

Dangerous Personal Property: Property with harmful potential such as weapons, ammunition, and dual-use property that can be converted to terrorist usage. Dangerous property will be

subject to life cycle management, which is to be tracked from acquisition to disposal.

Depreciation: The systematic rational allocation and periodic accounting entries made in the financial records to reflect decreases in the value of property through age, wear, deterioration, or obsolescence over its estimated useful life.

Destruction or Abandonment: The process used for ultimate disposal of personal property by ICE when no other means of disposal is appropriate.

Disposal: Any approved method used to remove an item from the property and financial records. Approved methods are: transferred to another agency or organizational element, sale, donation, abandonment, board of survey, and destruction.

Disposal Documents: Official forms used to adjust the property and the financial records.

E

Excess Personal Property: An asset identified as no longer required by an office that must be reported to the OCFO/OAA/Property Branch. Until the disposal is complete, excess items are accounted for.

Exchange/Sale Property: The process by which personal property not excess to the needs of ICE, but eligible for replacement, is exchanged or sold with the application of the allowance or proceeds towards purchase of the replacement item.

Expendable Personal Property: Property which, by its nature or function, is consumed in use, is used as repair parts or components of an end product considered non-expendable, or has an expected service life of less than one year.

F

Fair value: The price for which an asset could be bought or sold in an arm's-length transaction, an immediately available transaction, between unrelated parties (*e.g.*, between a willing buyer and a willing seller).

Federal Acquisition Regulation (FAR): The FAR contains the acquisition policies and procedures for Government agencies issued by GSA.

Federal Management Regulations (FMR): The successor regulation to the Federal Property Management Regulation (FPMR). The FMR contains updated regulatory policies originally found in the FPMR. However, it does not contain FPMR material that described how to do business with the GSA.

Federal Property and Administrative Services Act of 1949: The act which most directly affects property management. This legislation (63 Stat. 378, P.L. 152), as amended, became effective on July 1, 1949.

Federal Property Management Regulation System (FPMR): FPMR serves to govern and guide Federal agencies in prescribing regulations, policies, procedures, and delegations of authority pertaining to the management of property and records, and other programs and activities of the type administered by GSA, except procurement and contract matters contained in the Federal Acquisition Regulation (FAR).

Federal Register: A publication issued daily except Saturdays, Sundays, and legal holidays which contains proposed, general and permanent rules of all agencies of the Federal Government.

Federal Supply Schedule: A contract entered into by GSA with a vendor from which ordering agencies submit purchase orders for specified products.

Foreign Gifts and Donations: Gifts received and accepted from individuals representing a foreign government. A foreign gift which is accepted immediately becomes property of the Federal Government.

G

General Ledger: The fiscal record maintained by the OCFO/OFM which is comprised of several control accounts that reflect the dollar values of assets on hand. The general ledger is the primary record against which all property records are balanced.

Government Furnished Equipment: Any property, regardless of value, in the possession or control of a contractor which was directly acquired by ICE and subsequently furnished to the contractor, or acquired by the contractor with title vested in ICE. Government Furnished Equipment is provided to a contractor under the terms and conditions outlined in a contract.

Gross Negligence: An act or omission of the employee(s) which constitutes misconduct, willful negligence, or a wanton and reckless disregard for the property.

H

Hazardous Property: Personal property components or material that is deemed hazardous, chemical substances or mixtures, or hazardous waste under the Hazardous Materials Transportation Act (HMTA), the Resource Conservation and Recovery Act (RCRA), or the Toxic Substances Control Act (TSCA). Such items are recognized by Material Safety Data Sheets or Hazardous Material Information Sheets. This property is subject to life-cycle management.

I

Idle Property: Personal property that is no longer needed by the organization to which it is assigned, no effort has been made to excess, and has not been reported to GSA.

Inventory: The formal listing (property record) of all personal property assigned to an organization.

Inventory Adjustments: Changes made to the official property record when physical counts and official records do not agree. All such changes require specific approval and a documentation trail specific to the type of adjustment for audit purposes.

L

Life-Cycle Management: The accounting of personal property is a continuous process from the time of planning and acquisition until the ultimate consumption or disposal of the property.

Life Expectancy: The number of years that an item of equipment can be anticipated to provide useful service when properly maintained.

Line Item: A single line entry on a reporting form which indicates a quantity of personal property at any one location that has the same description, condition code, and unit cost.

M

Maintenance: The act of cleaning, servicing, and repairing equipment to ensure that items are in operational condition.

N

Non-Capitalized Personal Property: All Government-owned personal property that does not meet the GAO or the holding agency's established criteria for capitalization and entry into the general ledger of the agency's financial management account.

Non-Expendable Personal Property: Property which is complete within itself, does not lose its identity or become a component part of another article when put into use and is of a durable nature with an expected service life of one year or more.

Non-Reportable Personal Property: Property which does not meet the reporting criteria set forth in FPMR 101-43.311, and therefore is not required to be formally reported to GSA, but which is available locally for transfer.

O

Original Cost: The initial cost of a property in the hands of its present owner. Not necessarily the cost to the property's first owner.

P

Personal Custody: An article which is "sensitive to appropriate for private use," or is used in situations beyond normal supervisory observation. Such property should be accounted for by the

person to whom use and trust of the item is assigned.

Personal Property: Property in use or controlled by ICE or any type or interest therein, except real and related property and records of the Federal Government. For management and accounting control, personal property is categorized as “expendable personal property,” “non-expendable-property,” and “controlled personal property.”

Personal Property Management: All functions necessary for the proper determination of need, source, acquisition, receipt, accountability, utilization, maintenance, rehabilitation, storage, distribution, and disposal of personal property.

Physical Inventory: A physical count of items for the purpose of verifying the actual items on hand against those recorded on the personal property record. A physical inventory consists of sighting, viewing, barcoding, or otherwise marking, determining condition, describing, reconciling of exceptions, recording, and reporting inventory completion.

Property, Plant, and Equipment (PP&E): Tangible assets that have an estimated useful life of two years or more, are not intended for sale in the ordinary course of operations, and have been acquired or constructed with the intention of being used or made available for use by the organization. PP&E also includes real property that is covered under DHS Management Directive 0560.

Purchase Order: An offer by the Government to buy certain property or non-personal services from commercial sources, upon specified terms and conditions.

R

Receiving Report: A property accounting (tracking) record which acknowledges receipt by an accountable individual of property or service from a vendor or other source.

Reconciliation: The process by which the OCFO/OAA/Property Branch reviews certified inventories to identify adjustments for complete accuracy, *e.g.*, changes, additions, deletions; and ensure the presence of supporting documentation and reports of survey (where applicable).

Replacement Standards: The factors that should be considered in making a decision to acquire new equipment.

Report of Survey: A Report of Survey is an official report prepared on a standardized form, which records the circumstance concerning the loss, damage or destruction of property and which serves as the authorization to relieve the Agency/program of accountability. Reports of Survey should be used as a last resort to close the status of an asset that has been lost, damaged or destroyed. A Report of Survey documents every effort that was made to locate or resolve an asset. This process includes removing the asset from Sunflower.

Reportable Property: Personal property which is required to be reported to the General Services Administration (GSA) in accordance with FMR 102-36.210 prior to disposal. This

promotes reuse by the Government to enable Federal agencies to benefit from the continued use of property already paid for with taxpayer's money, thus minimizing new procurement costs. Reporting excess personal property to GSA helps ensure that the information on available excess personal property is accessible and disseminated to the widest range of customers.

Risk Assessment: A documented review by management of a component's degree of susceptibility to waste, loss, unauthorized use, or misappropriation and includes consideration of management controls.

S

Salvage: Property which has some value in excess of its basic material content, but is in such condition that it has no reasonable prospect of use for the purpose originally intended, and its repair or rehabilitation for use is impractical.

Scrap: Property that has no value except for its basic material content.

Seized Property: Personal property that has been confiscated by a Federal agency, and whose care and handling will be the responsibility of that agency until final ownership is determined by the judicial process.

Sensitive Personal Property: All items, regardless of value, that require special control and accountability due to unusual rates of loss, theft or misuse, or due to national security or export control considerations. Such property includes weapons, ammunition, explosives, information technology equipment with memory capability, cameras, and communications equipment. These classifications do not preclude agencies from specifying additional personal property classifications to effectively manage their Programs.

Simple negligence: The failure or omission to observe, for the protection of Government interest, that degree of care, precaution and vigilance, whereby the Government suffers through loss, damage, or destruction of property.

Source Documentation: Documentation that justifies adjustments in Sunflower. Source Documents may include Purchase Orders or other acquisition documents, SF-120s (Report of Excess Personal Property), and Certificate of Disposal (see Appendix C Forms).

State Agency for Surplus Property: An agency in each State designated under State law as responsible for the fair and equitable distribution, within the State, of all donations of surplus personal property to public agencies and eligible non-profit, tax-exempt activities for authorized purposes.

Sunflower Asset Management System (Sunflower): ICE's automated personal property management system. The system should contain a record for each piece of personal property subject to physical inventory. Sunflower is a commercial off-the-shelf (COTS) software program designed to manage assets within various organizational elements of DHS and to provide a wide range of functional capabilities in the lifecycle management of its assets.

Surplus Personal Property: Excess personal property not required for the needs and the discharge of the responsibilities of all Federal agencies, as determined by GSA.

U

Unclaimed (or Abandoned Property): Personal property that is found on premises owned or leased by ICE and is subject to the filing of a claim by the former owner within 3 years of vesting of title in the United States.

Usable Property: A disposable Condition Code that describes property other than scrap and waste.

Use Standard: Guideline established for determining in what quantity, when, and where items or categories of items are required.

Utilization: The identification, reporting and transfer of excess personal property among Federal agencies to fill current or future authorized requirements in lieu of new procurement.

W

Willful Intent: The determination made by a Board of Survey to describe someone willfully damaging or destroying personal property.

(Program Office Name)

U.S. Department of Homeland Security

(Program Office Address Line 1)

(Program Office Address Line 2)



**U.S. Immigration
and Customs
Enforcement**

Appendix A: PC Designation Letter

MEMORANDUM FOR (Program Office Name) Employees

FROM: (APO Name)

Accountable Property Officer

SUBJECT: Appointment as Property Custodian

Ref: (a) Personal Property Operations Handbook
(b) Office of Asset Administration Webpage
(c) Office of Asset Administration SOP No: OAA/PROP 00006

1. In accordance with references (a) and (b), you are hereby appointed as Property Custodian for all (Program Office Name) property that is under your Custodial Steward Code: (Steward Code and Group). As Custodian, you will be responsible for the accountability and safeguarding of accountable property, and accuracy of information recorded in Sunflower.

2. As the Property Custodian, your responsibilities include, but are not limited to: Ensuring that all computers under your administrative control are encrypted; reviewing all procurement requests for property; safeguarding sensitive equipment such as laptop computers, blackberries, and thumb drives; ensuring property is recorded in Sunflower within 5 working days of receiving the property; ensuring that all property, which no longer meets the operational requirement of ICE, is reported as excess and disposed of properly; coordinating Reports of Survey for property lost, stolen, or damaged; coordinating the search for missing property; maintaining property management files and supporting documentation to support and substantiate the information recorded in Sunflower including assigning property to users and ensuring user, location, and accountability for the asset is accurate/up-to-date.

3. A physical inventory of all Personal Property is required every year, in accordance with references (a) and (b), and upon relief of the custodian. Inventories may be taken more frequently than required, if deemed necessary by the APO/EAD/AD/Office Manager. I will designate other staff to conduct periodic physical inventories of property based on guidance from the ICE Property Management Officer. You will assist as needed in those inventories and prepare inventory packages for my review and forward to the Headquarters Program Property Officer.

4. For a more comprehensive list of responsibilities and guidance, refer to references (a) and (b).

Copy to: (HPPM Name)

(Program Office) – HPPM

(Program Office Name)

U.S. Department of Homeland Security

(Program Office Address Line 1)

(Program Office Address Line 2)



U.S. Immigration
and Customs
Enforcement

Appendix B: HPPM Designation Letter

MEMORANDUM FOR (Program Office Name) Employees

FROM: (APO Name)

Accountable Property Officer

SUBJECT: Appointment as Headquarters Program Property Manager

Ref: (c) Personal Property Operations Handbook
(d) Office of Asset Administration Webpage

1. In accordance with references (a) and (b), you are hereby appointed as Headquarters Program Property Manager (HPPM) for all (Program Office Name) property that is under the Parent Steward Code: (Steward Code and Group). As HPPM, you have oversight for your area of jurisdiction to ensure an accurate accounting of all program property. Serve as liaisons between (Program Office Name) and the Office of Asset Administration (OAA) Property Branch, to coordinate property matters, and are considered the Subject Matter Experts for (Program Office Name).

2. As the HPPM, your responsibilities include, but are not limited to: Overseeing and administering property management responsibilities. Ensuring that offices comply with established deadlines for inventory, recording property transactions, and reporting. Serving as the first-level of property management support to Property Custodians (PC). Facilitating, coordinating, and compiling supporting documentation for property transactions upon request. Verifying the accuracy of supporting documentation before submission to the Property Branch. Submitting monthly ROS, including negative reports (reporting that there are no ROS) to the Property Branch. Ensuring that property personnel are aware of and register for required property management training. Monitoring and managing their Program's personal property inventory. Ensuring timely maintenance of property records for transactions including acquisitions, transfers, and disposals of personal property. Performing quality assurance reviews of property records. Disseminating property related communications within their program. Disseminating and reinforcing all communication sent from the Property Branch to Program Offices.


3. For a more comprehensive list of responsibilities and guidance, refer to references (a) and (b).

Copy to: OAA Property Branch

Appendix C: Forms


Form	Form Name
Certificate of Excess Screening	Certificate of Excess Screening
ICE Form 12-023	Certificate of Disposal
Certificate of HD Clean	Certificate of HD Clean
DHS 560-3	DHS Property Transfer Receipt
G-504	ICE Report of Property Shipped - Received
G-514	ICE Purchase Requisition
G-570	ICE Record of Receipt-Property Issued to Employee
G-574	ICE Property Control Card for Temporary Issues
SF-120	GSA Report of Excess Personal Property
SF-122	GSA Transfer Order Excess Personal Property
SF-123	GSA Transfer Order Surplus Personal Property
SF-126	GSA Report of Personal Property for Sale

Certificate of Excess Screening

 U.S. Immigration and Customs Enforcement		Certificate of Excess Screening		
		REPORT NUMBER AAC-Julian Date-Log #		
NAME ICESTUDENT01		DATE 8/12/08		
TITLE Property Custodian		PHONE NUMBER		
OFFICE		ORGANIZATION CODE ICESTW01		
LINE ITEM	DESCRIPTION OF PROPERTY <i>(Include make, model, serial number, barcode number)</i>	QUANTITY	UNIT VALUE	TOTAL VALUE
I certify that I have made positive efforts to satisfy the ICE property requirements described herein by obtaining and using excess personal property before initiating any other form of acquisition in accordance with Subpart 8.1 of the FAR regulations.				
PROPERTY CUSTODIAN		ACCOUNTABLE PROPERTY OFFICER		
NAME		NAME		
SIGNATURE		SIGNATURE		

(This form is currently under review from ICE OPLA and Privacy for formal forms approval process)

Certificate of Disposal

 U.S. Immigration and Customs Enforcement		<h2>Certificate of Disposal</h2>			
NAME ICESTUDENT01 TITLE Property Custodian OFFICE		DATE 8/12/08 PHONE NUMBER ORGANIZATION CODE ICESTW01			
REPORT NUMBER AAC-Julian Date-Log #		DATE TRANSFER, DONATION, SALE, ABANDONMENT, OR DESTRUCTION COMPLETED Date the transfer/donation/sale/abandonment/destruction was completed			
LINE ITEM NUMBER	DESCRIPTION OF PROPERTY	BAR CODE NUMBER	SALES PROCEEDS	SALES FEES	SALES AMT. TO ICE
0001	Dell Computer GX620, S/N 23490	CS26410	How much received from sale \$600	Fees applied \$100	How much \$ ICE received from sale \$500
NAME OF AGENCY/PURCHASER		ADDRESS AND TELEPHONE NUMBER	DATE PROPERTY PICKED UP OR SHIPPED	ADPE SANITIZED YES/NO N/A	
METHOD OF ABANDONMENT/DESTRUCTION How property was destroyed (UNICOR,			LOCATION OF ABANDONMENT/DESTRUCTION Location where the property was destroyed or abandoned. List address		
DONATION (NAME AND ADDRESS)					
WITNESS #1			WITNESS #2		
NAME			NAME		
SIGNATURE			SIGNATURE		
ICE PERSONNEL COMPLETING CERTIFICATE OF DISPOSAL					
NAME			SIGNATURE		
TITLE					
RECIPIENT OF ITEM(S)					
NAME			SIGNATURE		
TITLE			AGENCY/COMPANY		

(This form is currently under review from ICE OPLA and Privacy for formal forms approval process)

*This also includes vehicles

Certificate of HD Clean


SECURITY INSPECTION AND RELEASE AUTHORITY						
INSTRUCTIONS						
Complete Part 1 of this form to document the local release or disposal of any component (such as a printer) or sub-component (such as a printed circuit board) being removed from any information system. File a copy of the completed form with the Accreditation Package. If the form is used to release a complete information system for which the accreditation has to be formally rescinded and components formally released, forward the signed hard copy original form and a soft copy to the Information Systems Security Branch (ISSB).						
PART I. TO BE COMPLETED BY THE CSO OR EQUIPMENT CUSTODIAN						
1. Type or print name and title [REDACTED]			2. Grade [REDACTED]		3. Date [REDACTED]	
4. Organization, Office, return mailing address [REDACTED]					5. Office phone number [REDACTED]	
6. Has the equipment processed sensitive or classified information? [REDACTED]					<input type="checkbox"/> YES	<input type="checkbox"/> NO
7. Does the equipment contain electronic or magnetic storage capability? [REDACTED]					<input type="checkbox"/> YES	<input type="checkbox"/> NO
8.	Has the equipment been physically searched for sensitive or classified material? [REDACTED]				<input type="checkbox"/> YES	<input type="checkbox"/> NO
	Was an incident report initiated if sensitive or classified information was found? [REDACTED]				<input type="checkbox"/> YES	<input type="checkbox"/> NO
9.	Was the equipment degaussed? [REDACTED]				<input type="checkbox"/> YES	<input type="checkbox"/> NO
	If YES, provide the name, model, and date of the calibration of the degausser. [REDACTED]					
10.	Was the equipment overwritten? (if YES, attach a description of the overwrite procedure) [REDACTED]				<input type="checkbox"/> YES	<input type="checkbox"/> NO
11. System name on Accreditation Package [REDACTED]			12. Reason for release [REDACTED]			
13. Enter all items to be released						
MODEL		DESCRIPTION		SERIAL NUMBER	IDENTIFY ACTION	
					DESTROY	DEGAUSS
					OVERWRITE	
					<input type="checkbox"/>	<input type="checkbox"/>
					<input type="checkbox"/>	<input type="checkbox"/>
					<input type="checkbox"/>	<input type="checkbox"/>
					<input type="checkbox"/>	<input type="checkbox"/>
					<input type="checkbox"/>	<input type="checkbox"/>
					<input type="checkbox"/>	<input type="checkbox"/>
Comments: [REDACTED]						
15. Signature if individual in Part 1. [REDACTED]				16. Signature of the Organization's Information Systems Security Officer [REDACTED]		
PART II. TO BE COMPLETED BY THE INFORMATION SYSTEMS SECURITY MANAGER- The accreditation of this system (item 1) is formally rescinded once this form is signed by the ISSM. This signature authorized the release or disposal of the equipment in item 13.						
17. Signature of Information Systems Security Manager [REDACTED]						18. Date [REDACTED]

U.S. CUSTOMS FORM 2001

SECURITY CLASSIFICATION (IF ANY)

[illegible]

G-504 ICE Report of property Shipped – Received

 U.S. Immigration and Customs Enforcement		Type of Transfer		Report Number AAC-Julian Date- Log #	
<i>Report of Property Shipped - Received</i>		<div style="display: flex; justify-content: space-around;"> <div style="text-align: center;"> <input type="checkbox"/> Permanent <input type="checkbox"/> Transfer </div> <div style="text-align: center;"> <input type="checkbox"/> Temporary <input type="checkbox"/> Loan </div> </div>		Page _____ of _____ Date Date form created Authorized Official Signature APO Signature POC Telephone Number APO Phone #	
TRANSFERRED FROM Office Property is being transferred FROM				Estimated return date if temporary: Fill out if transfer is LOAN	
TRANSFERRED TO Office Property is being transferred TO					
Instructions or Remarks: Location Property is Going To, Coming From, anything else important					
Item No. (1)	Description (2)	Bar Code Number (3)	Serial Number (4)	Unit of Issue (5)	Original Cost (6)
Each item gets own item number starting with 0001 0001	Descriptions should be brief but complete Example: Dell Computer GX240, Model.12345, Computer works but has bad video card	CS123456	AB11XYZ	1	\$1,500
Shipped by Date Signature and Title APO or Delegate		Received by Date Signature and Title A P O or D e l e g a t e			

G-514 ICE Purchase Requisition

REQUISITION — MATERIALS-SUPPLIES-EQUIPMENT				1. NUMBER DRO-04-RQ0029		
SEE INSTRUCTIONS ON REVERSE				2. DATE 28-MAY-2004		
SEE INSTRUCTIONS ON REVERSE				3. ACTIVITY SYMBOL See Attachment A		
4. TO: NAME AND ADDRESS — PROCUREMENT SECTION (OR STOREROOM) DHS PROCUREMENT OFFICE 24000 AVILA ROAD LAGUNA NIGUEL, CA 92677			5. FROM: NAME AND ADDRESS — REQUISITIONER DHS, ICE, E&LR BRANCH DIANE SIMON 24000 AVILA ROAD, # 5180 LAGUNA NIGUEL, CA 92677			
STOCK NUMBER	DESCRIPTION OF ARTICLE (MAKE, MODEL, TYPE, SIZE, COLOR, MFG., ETC)	QUANTITY	UNIT	COST		ACTION CODE
				UNIT PRICE	AMOUNT	
6	7	8	9	10	11	12
	DOCUMENT MAILING FEE	1	EA	20.00	20.00	
	EST. FEE AND COST FOR COURT REPORTER TRANSCRIPTION SERVICES	5	EA	400.00	2,000.00	
	COURT REPORTER APPEARANCE FEE FOR 1-DAY	1	EA	150.00	150.00	
Justification: COURT REPORTER NEEDED FOR ARBITRATION HEARING FOR EMPLOYEE ROBYN PERRY Recommended Vendor: 521097058 NEAL R GROSS & CO INC CCR DATA IN SYSTEM WASHINGTON, DC 20005-3701 Phone: (202) 234-4433 Contact: NEAL GROSS						
13. SIGNATURE OF APPROVING OFFICIAL			14. TITLE OF APPROVING OFFICIAL			
24. SIGNATURE OF FUNDING OFFICIAL G K SOURK			25. TITLE OF FUNDING OFFICIAL		15. TOTAL 2,170.00	
16. KEY TO ACTION CODE				17. DATE RECEIVED		
9 SUBSTITUTE ITEM 0 BACK ORDERED 0 PURCHASED FOR DIRECT SHIPMENT 1 CANCELLED—STOCK EXHAUSTED				18. PURCHASE ORDER DATE NUMBER 16. APPROVED		
I CERTIFY THAT THE ABOVE ARTICLES — COLUMNS 3, 9 AND 12 — HAVE BEEN RECEIVED.						
20. LOCATION		21. DATE		22. SIGNATURE		23. TITLE

United States Department Of Homeland Security
 Immigration And Customs Enforcement
 FORM G-514 (REV. 8-1-5)

Page 1 of 3

G-570 ICE Record of Receipt-Property Issues to Employee

1. Employee Name and Title Purpose of Issued Property:					2. Location/Program	
	PROPERTY		RECEIVED		RETURNED	
3. Quantity	4. Description	5. Serial No.	6. Date	7. Employee's Signature	8. Date	9. Supervisor's Signature

G-574 ICE Property Control Card for Temporary Issues

DESCRIPTION		BARCODE #		OFFICE
RADIO <input type="checkbox"/> WEAPON <input type="checkbox"/> OTHER <input type="checkbox"/>				
DATE ISSUED	ISSUED TO SIGNATURE	DATE RETURNED	RECEIVED BY SIGNATURE	

SF-120 GSA Report of Excess Personal Property

STANDARD FORM 120 REV. APRIL 1957 GEN. SERV. ADMIN. FPMR (41 CFR) 101-		REPORT OF EXCESS PERSONAL PROPERTY		1. REPORT NO. AAC-0231-0008		2. DATE MAILED 8/20/08		3. TOTAL COST \$ 1464.00	
4. TYPE (Check "a," "b," "c," "d," "e," "f," "g," "h," "i," "j," "k," "l," "m," "n," "o," "p," "q," "r," "s," "t," "u," "v," "w," "x," "y," "z," "aa," "ab," "ac," "ad," "ae," "af," "ag," "ah," "ai," "aj," "ak," "al," "am," "an," "ao," "ap," "aq," "ar," "as," "at," "au," "av," "aw," "ax," "ay," "az," "ba," "bb," "bc," "bd," "be," "bf," "bg," "bh," "bi," "bj," "bk," "bl," "bm," "bn," "bo," "bp," "bq," "br," "bs," "bt," "bu," "bv," "bw," "bx," "by," "bz," "ca," "cb," "cc," "cd," "ce," "cf," "cg," "ch," "ci," "cj," "ck," "cl," "cm," "cn," "co," "cp," "cq," "cr," "cs," "ct," "cu," "cv," "cw," "cx," "cy," "cz," "da," "db," "dc," "dd," "de," "df," "dg," "dh," "di," "dj," "dk," "dl," "dm," "dn," "do," "dp," "dq," "dr," "ds," "dt," "du," "dv," "dw," "dx," "dy," "dz," "ea," "eb," "ec," "ed," "ee," "ef," "eg," "eh," "ei," "ej," "ek," "el," "em," "en," "eo," "ep," "eq," "er," "es," "et," "eu," "ev," "ew," "ex," "ey," "ez," "fa," "fb," "fc," "fd," "fe," "ff," "fg," "fh," "fi," "fj," "fk," "fl," "fm," "fn," "fo," "fp," "fq," "fr," "fs," "ft," "fu," "fv," "fw," "fx," "fy," "fz," "ga," "gb," "gc," "gd," "ge," "gf," "gg," "gh," "gi," "gj," "gk," "gl," "gm," "gn," "go," "gp," "gq," "gr," "gs," "gt," "gu," "gv," "gw," "gx," "gy," "gz," "ha," "hb," "hc," "hd," "he," "hf," "hg," "hh," "hi," "hj," "hk," "hl," "hm," "hn," "ho," "hp," "hq," "hr," "hs," "ht," "hu," "hv," "hw," "hx," "hy," "hz," "ia," "ib," "ic," "id," "ie," "if," "ig," "ih," "ii," "ij," "ik," "il," "im," "in," "io," "ip," "iq," "ir," "is," "it," "iu," "iv," "iw," "ix," "iy," "iz," "ja," "jb," "jc," "jd," "je," "jf," "jg," "jh," "ji," "jj," "jk," "jl," "jm," "jn," "jo," "jp," "jq," "jr," "js," "jt," "ju," "jv," "jw," "jx," "jy," "jz," "ka," "kb," "kc," "kd," "ke," "kf," "kg," "kh," "ki," "kj," "kk," "kl," "km," "kn," "ko," "kp," "kq," "kr," "ks," "kt," "ku," "kv," "kw," "kx," "ky," "kz," "la," "lb," "lc," "ld," "le," "lf," "lg," "lh," "li," "lj," "lk," "ll," "lm," "ln," "lo," "lp," "lq," "lr," "ls," "lt," "lu," "lv," "lw," "lx," "ly," "lz," "ma," "mb," "mc," "md," "me," "mf," "mg," "mh," "mi," "mj," "mk," "ml," "mm," "mn," "mo," "mp," "mq," "mr," "ms," "mt," "mu," "mv," "mw," "mx," "my," "mz," "na," "nb," "nc," "nd," "ne," "nf," "ng," "nh," "ni," "nj," "nk," "nl," "nm," "nn," "no," "np," "nq," "nr," "ns," "nt," "nu," "nv," "nw," "nx," "ny," "nz," "oa," "ob," "oc," "od," "oe," "of," "og," "oh," "oi," "oj," "ok," "ol," "om," "on," "oo," "op," "oq," "or," "os," "ot," "ou," "ov," "ow," "ox," "oy," "oz," "pa," "pb," "pc," "pd," "pe," "pf," "pg," "ph," "pi," "pj," "pk," "pl," "pm," "pn," "po," "pp," "pq," "pr," "ps," "pt," "pu," "pv," "pw," "px," "py," "pz," "qa," "qb," "qc," "qd," "qe," "qf," "qg," "qh," "qi," "qj," "qk," "ql," "qm," "qn," "qo," "qp," "qq," "qr," "qs," "qt," "qu," "qv," "qw," "qx," "qy," "qz," "ra," "rb," "rc," "rd," "re," "rf," "rg," "rh," "ri," "rj," "rk," "rl," "rm," "rn," "ro," "rp," "rq," "rr," "rs," "rt," "ru," "rv," "rw," "rx," "ry," "rz," "sa," "sb," "sc," "sd," "se," "sf," "sg," "sh," "si," "sj," "sk," "sl," "sm," "sn," "so," "sp," "sq," "sr," "ss," "st," "su," "sv," "sw," "sx," "sy," "sz," "ta," "tb," "tc," "td," "te," "tf," "tg," "th," "ti," "tj," "tk," "tl," "tm," "tn," "to," "tp," "tq," "tr," "ts," "tt," "tu," "tv," "tw," "tx," "ty," "tz," "ua," "ub," "uc," "ud," "ue," "uf," "ug," "uh," "ui," "uj," "uk," "ul," "um," "un," "uo," "up," "uq," "ur," "us," "ut," "uu," "uv," "uw," "ux," "uy," "uz," "va," "vb," "vc," "vd," "ve," "vf," "vg," "vh," "vi," "vj," "vk," "vl," "vm," "vn," "vo," "vp," "vq," "vr," "vs," "vt," "vu," "vv," "vw," "vx," "vy," "vz," "wa," "wb," "wc," "wd," "we," "wf," "wg," "wh," "wi," "wj," "wk," "wl," "wm," "wn," "wo," "wp," "wq," "wr," "ws," "wt," "wu," "wv," "ww," "wx," "wy," "wz," "xa," "xb," "xc," "xd," "xe," "xf," "xg," "xh," "xi," "xj," "xk," "xl," "xm," "xn," "xo," "xp," "xq," "xr," "xs," "xt," "xu," "xv," "xw," "xx," "xy," "xz," "ya," "yb," "yc," "yd," "ye," "yf," "yg," "yh," "yi," "yj," "yk," "yl," "ym," "yn," "yo," "yp," "yq," "yr," "ys," "yt," "yu," "yv," "yw," "yx," "yy," "yz," "za," "zb," "zc," "zd," "ze," "zf," "zg," "zh," "zi," "zj," "zk," "zl," "zm," "zn," "zo," "zp," "zq," "zr," "zs," "zt," "zu," "zv," "zw," "zx," "zy," "zz")		a. ORIGINAL <input checked="" type="checkbox"/>		c. PARTIAL W/D (Also check "e" and/or "f" if appropriate)		e. OVERSEAS <input type="checkbox"/>		f. CONTRACTORS <input type="checkbox"/>	
5. TO (Name and Address of Agency to which report is made) THRU ICE HQ OCFO/OAA Attn: (b) (6), (b) (7)(C) 50012th ST SW, Washington, DC 20536					6. APPROP. OR FUND TO BE REIMBURSED (if any)				
7. FROM (Name and Address of Reporting Agency) (b) (6), (b) (7)(C) 425 I St., NW, Washington DC, 20536 202-555- (b) (6), (b) (7)(C) 202-569- (b) (6), (b) (7)(C)					Accountable Property Officer (SAC, FOD, etc.) APO Signature				
9. FOR FURTHER INFORMATION CONTACT (Title, Address and Telephone No.) Program Point of Contact, Address and Phone Number					10. AGENCY APPROVAL (If applicable) APO Signature				
11. SEND PURCHASE ORDERS OR DISPOSAL INSTRUCTIONS TO (Title, Address and Telephone No.) N/A					12. GSA CONTROL NO.				
13. FSC GROUP NO.		14. LOCATION OF PROPERTY (If location is to be abandoned give date) (b) (6), (b) (7)(C) 425 I St., NW Washington, DC 20536		15. REIM/REQD YES <input type="checkbox"/> NO <input type="checkbox"/>		16. AGENCY CONTROL NO.		17. SURPLUS RELEASE DATE TBD or leave blank	
18. EXCESS PROPERTY LIST		COND. (c)	UNIT (d)	NUMBER OF UNITS (e)	ACQUISITION COST		FAIR VALUE % (h)		
ITEM NO. (a)	DESCRIPTION (b)				PER UNIT (f)	TOTAL (g)			
0001	Dell Computer 1400SC ICE Computer's hard drive no	7	EA	1	\$1,464	\$1,464.00			
0002	(Manufacturer, Model, Serial # Barcode)								

STANDARD FORM
120 REV.
APRIL 1957
EDITION

(Use Standard Form 120A for Continuation Sheets)

120-104

SF-122 GSA Transfer Order Excess Personal Property

STANDARD FORM 122 JUNE 1974 GENERAL SERVICES ADMINISTRATION FPMR (41 CFR) 101-2.306 FPMR (41 CFR) 101-3.315		TRANSFER ORDER EXCESS PERSONAL PROPERTY			1. ORDER NO. Report Number AAC-Julian Date- Log #	
		2. DATE Date form is created				
3. TO: General Services Administration* The Address for GSA in your Region				4. ORDERING AGENCY (Full name and address)* Agency receiving the Property		
5. HOLDING AGENCY (Name and address)* APO's Name, Address, Phone and Fax Numbers				6. SHIP TO (Consignee and destination)* Only complete if Address is different from above If same, put "Same as Block 4"		
7. LOCATION OF PROPERTY Address of where property is physically located				8. SHIPPING INSTRUCTIONS How the property was shipped		
9. ORDERING AGENCY APPROVAL						
a. SIGNATURE Person receiving the property		b. DATE Date property was received		Leave Blank Use only for reimbursements		
c. TITLE Title of person receiving property				11. ALLOTMENT Leave Blank		12. GOVERNMENT B/L NO. Leave Blank
13. PROPERTY ORDERED						
GSA AND HOLDING AGENCY NOS. (a)	ITEM NO. (b)	DESCRIPTION (Include noun name FSC Group and Class. Condition code and if available, National Stock Number) (c)	UNIT (d)	QUANTITY (e)	ACQUISITION COST	
					UNIT (f)	TOTAL (g)
Barcode Number	0001		EA	2	\$1,500	\$3,000
14. GSA APPROVAL		a. SIGNATURE Leave for GSA		b. TITLE		c. DATE
FOR	AGENCY & LOCATION					
GSA USE ONLY	AGENCY	STATE	FSC	CONDITION	SOURCE CODE	

SF-123 GSA Transfer Order Surplus Personal Property

TRANSFER ORDER SURPLUS PERSONAL PROPERTY		1. ORDER NUMBER(S) a. _____ b. _____		FORM APPROVED OMB NUMBER 3090-0014		PAGE 1 OF PAGES	
2. TYPE OF ORDER <input type="checkbox"/> STATE AGENCY <input type="checkbox"/> DOD(SEA) <input type="checkbox"/> FAA		3. SURPLUS RELEASE DATE		4. SET ASIDE DATE		5. <input type="checkbox"/> NON-REPORTABLE <input type="checkbox"/> REPORTABLE	
6. TOTAL ACQUISITION COST		7. TO GENERAL SERVICES ADMINISTRATION* The address for GSA in their region					
8. LOCATION OF PROPERTY If different than block 9		9. HOLDING AGENCY (Name and Address)* Name and address of Agency who has the property					
10. FOR GSA USE ONLY		SOURCE CODE <input type="checkbox"/> STATE <input type="text"/> <input type="text"/> CITY <input type="text"/> <input type="text"/> <input type="text"/> TYPED OF DONATION <input type="text"/> ADJUSTED ALLOCATION CODE <input type="text"/>					
11. PICKUP OR SHIPPING INSTRUCTIONS*							
12. SURPLUS PROPERTY LIST							
L/I NO.	IDENTIFICATION NUMBER(S)	DESCRIPTION	DEMIL. CODE	COND. CODE	QUANTITY AND UNIT	ACQUISITION COST	
						UNIT	TOTAL
(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)
001	Barcode number	Make Model name, Model, and Serial Number	A	4	1	\$500	\$500
13. TRANSFEREE ACTION Transferee certifies and agrees that transfers and donations are made in accordance with 41 CFR 101-44, and to the terms, conditions, and assurances as specified on this document.		a. TRANSFEREE (Name and address of state Agency, SEA, or public airport)* Person receiving the item		b. SIGNATURE AND TITLE OF STATE AGENCY OR DONEE REPRESENTATIVE		c. DATE	
				d. SIGNATURE OF HEAD OF SEA (School or National Headquarters)		e. DATE	
14. ADMINISTRATIVE ACTION I certify that the administrative actions pertinent to this order are in accordance with 41 CFR 101-44 and as specified on this document have been and are being taken.		a. DETERMINING OFFICER (DOD OR FAA)*		b. SIGNATURE OF DETERMINING OFFICER		c. DATE	
		d. GSA APPROVING OFFICER		e. SIGNATURE OF APPROVING OFFICER		f. DATE	
*Please include "ZIP codes" in all address blocks. WHITE STANDARD FORM 123 (Rev6-82) NSN 7540-00-965-2415 (41 CFR) 101.44.110 Previous Editions not usable Prescribed by GSA FPMR							

SF-126 GSA Report of Personal Property for Sale

		Page 93	OF
1. FROM (name, address and zip code of owning agency) Office giving the property away		2. REPORT NO. AAC-Julian Date-log number	
		4. FSC GROUP 2310 (vehicle)	
		3. DATE Date form is completed	
5. TOTAL ACQUISITION COST Original purchase price			
6. PUBLIC MAY INSPECT PROPERTY BY CONTACTING (NAME, ADDRESS, ZIP CODE) Same as Block #1		7. PROPERTY LOCATED AT Where the property is physically located	
8. TO General Services Administration Region Contact Information		9.	
		a. ACTIVITY WILL LOAD FOR PURCHASER (If the office has the means to load the equipment) <input type="checkbox"/> (1) YES <input type="checkbox"/> (2) NO	
		b. EXTENT (if CHECKED "YES") (e.g. forklift or pallet jack)	
		10. PROPERTY IS EXCHANGE/SALE <input type="checkbox"/> a. YES <input type="checkbox"/> b. NO	
11. PROPERTY IS REIMBURSABLE (same answer as <input type="checkbox"/> a. YES <input type="checkbox"/> b. NO			
12. SEND EXECUTED SALES DOCUMENTS TO (NAME, ADDRESS AND ZIP CODE) Same as Block #1		13. DEPOSIT PROCEEDS TO (APPROPRIATE FUND SYMBOL AND TITLE) Account # specified by the Property office	
		14. STATION DEPOSIT SYMBOL OR STATION ACCOUNT NUMBER Leave blank	
15. UTILIZATION AND DONATION SCREENING REQUIREMENTS COMPLETED. PROPERTY IS AVAILABLE FOR SALE.		BY (SIGNATURE AND TITLE)	
PROPERTY LIST (USE CONTINUATION SHEET, IF NECESSARY)			
16.			
ITEM NO. (a)	ITEM NO. ASSIGNED BY GSA (b)	COMMERCIAL DESCRIPTION AND	UNIT (d)
			NUMBER OF UNITS (e)
			ACQUISITION COST
			PER UNIT
			TOTAL (g)
0001	Barcode Number		EA 2 \$1,500 \$3,000
17. RECEIPT OF PROPERTY AT GSA SALES SITE OR CENTER ACKNOWLEDGED		18. RECEIPT IS HEREBY ACKNOWLEDGED	
SIGNATURE AND TITLE Leave for GSA		DATE	
FOR GSA INTERNAL USE ONLY			
19. SALE NO.	20. TYPE OF SALE	21. INSPECTION DATES	22. BID OPENING DATE AND TIME

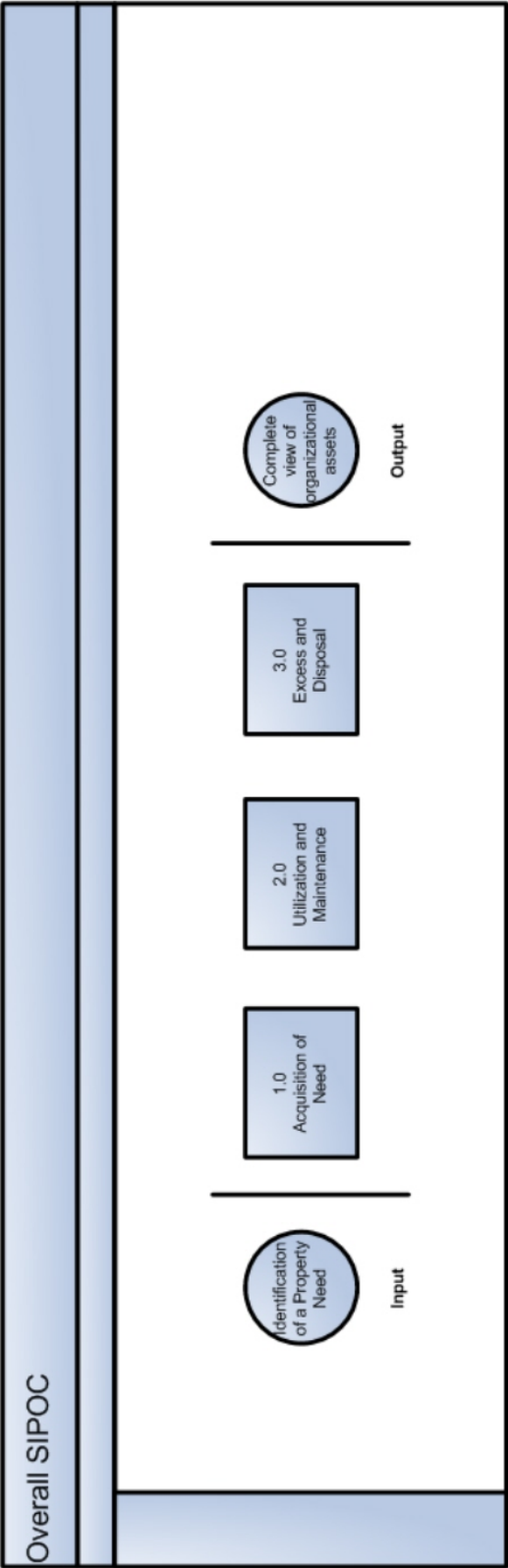
Appendix D: Acronym List

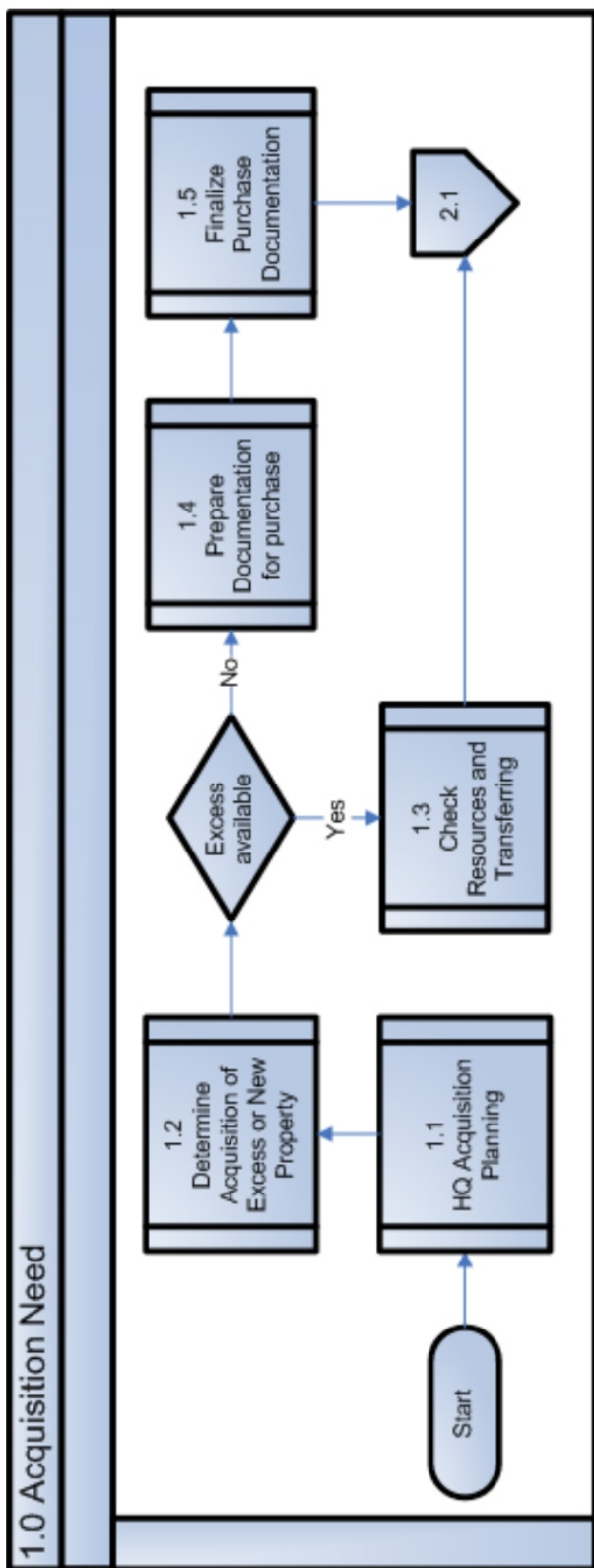
Acronym	Full Title	Acronym	Full Title
ACCS	Accounting Code Classification Structure	NFTTU	National Firearms and Tactical Training Unit
ADPE	Automated Data Processing Equipment	NUO	National Utilization Officer
APO	Accountable Property Officer	OAC	Office of Assurance and Compliance
ASB	Administrative Services Branch	OAA	Office of Asset Management
BFC	Burlington Finance Center	OAQ	Office of Acquisition
BOS	Board of Survey	OCFO	Office of The Chief Financial Officer
CFL	Computers for Learning Program	OCIO	Office of the Chief Information Officer
CO	Contracting Officer	OFM	Office of Financial Management
DASM	Deputy Assistant Secretary for Management	OMB	Office of Management and Budget
DFC	Dallas Finance Center	OPR	Office of Professional Responsibility
DHS	Department of Homeland Security	ORG	Operational Risk Group
DHS-560-3	DHS Property Transfer Receipt	PC	Property Custodian
EBOS	Executive Board of Survey	PCard	Purchase Card
ECSF	East Coast Staging Facility	PCN	Potomac Center North
FFMS	Federal Financial Management System	PMO	Property Management Officer
G-504	ICE Report of Property Shipped - Received	PPOH	Personal Property Operations Handbook
G-514	ICE Purchase Requisition	PR	Purchase Request
G-570	ICE Record of Receipt-Property Issued to Employee	RO	Receiving Officer
G-574	ICE Property Control Card for Temporary Issues	ROS	Report of Survey
GSA	General Services Administration	SAMS	Sunflower Asset Management System
GSAXcess	GSA asset management system	SF-120	GSA Report of Excess Personal Property
HD	Hard drive	SF-122	GSA Transfer Order Excess Personal Property
HPPM	Headquarters Program Property Manager	SF-123	GSA Transfer Order Surplus Personal Property
ICE	U.S. Immigration and Customs Enforcement	SF-126	GSA Report of Personal Property for Sale
HSI	Homeland Security Investigations	SFFAS	Statement of Federal Financial Accounting Standards
ITFO	Information Technology Field Operations	SOP	Standard Operating Procedure
LPC	Local Property Custodian	TIE	Technical Investigative Equipment
NBOS	National Board of Survey	TMF	Technical Maintenance Facility

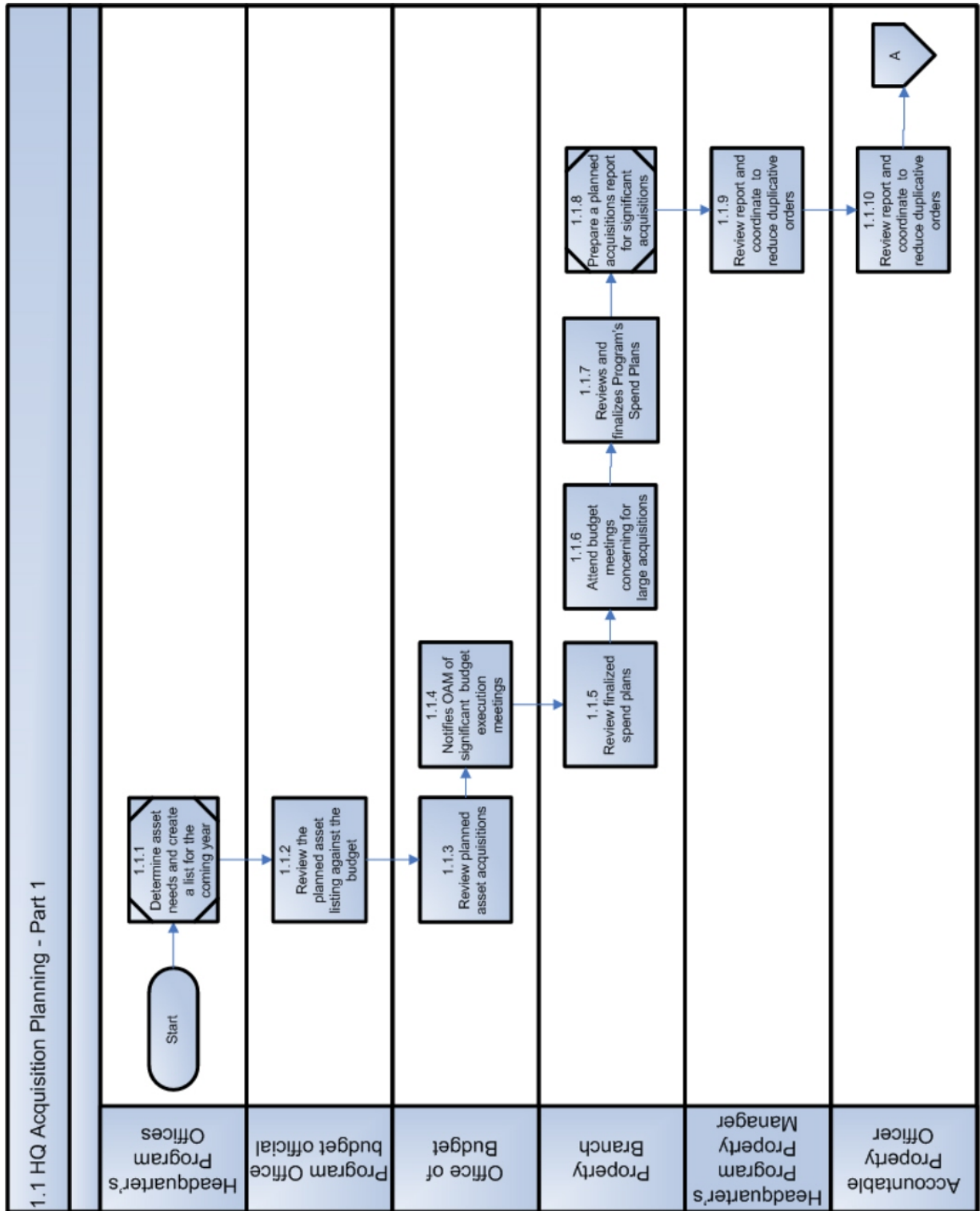
Appendix E: Process Flows with Key Control Matrices

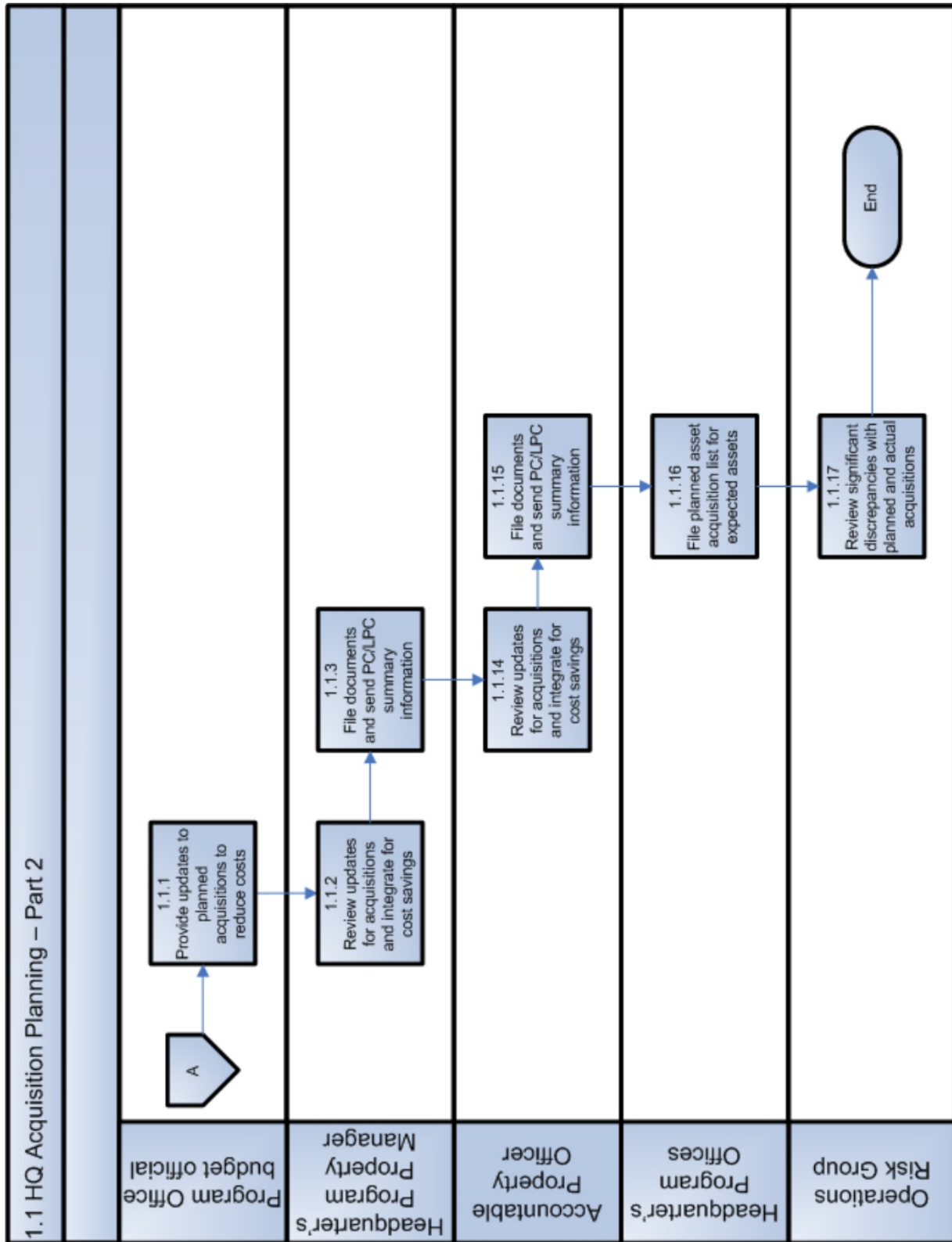
Process Flow Summary:

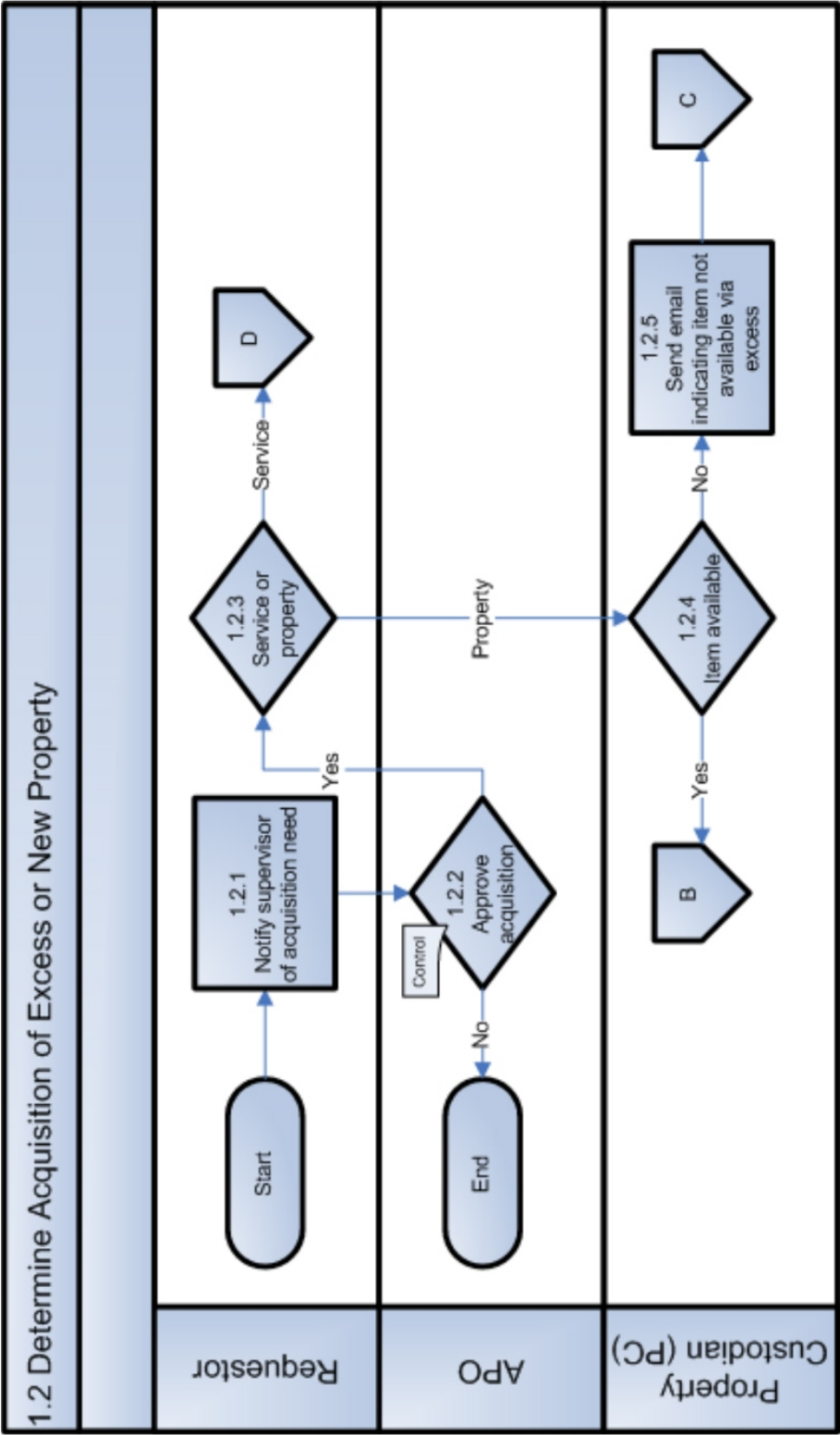
Life Cycle Component	Process Flow Title with Key Control Matrix
HQ Acquisition Planning	1. HQ Acquisition Planning
Acquiring Accountable Personal Property	1. Acquiring Excess Property 2. Acquiring Property through Procurement 3. Acquiring Property using a Purchase Card (PCard) 4. Leasing Property
Receiving and Barcode Labeling	1. Receiving and Barcode Labeling
Creating Property Records	1. Creating Property Records
Acquisition Costs and Values	1. Acquisition Costs and Values
Internal Transfers and Reassignments	1. Internal Transfers and Reassignments
The Inventory Process	1. The Inventory Process
Warehousing and Storage	1. Warehousing and Storage
Excess Screening	1. Excess Screening
Disposal	1. Disposal of Accountable Personal Property Through Donation 2. Disposal of Property through Sales 3. Disposal through Abandonment or Destruction

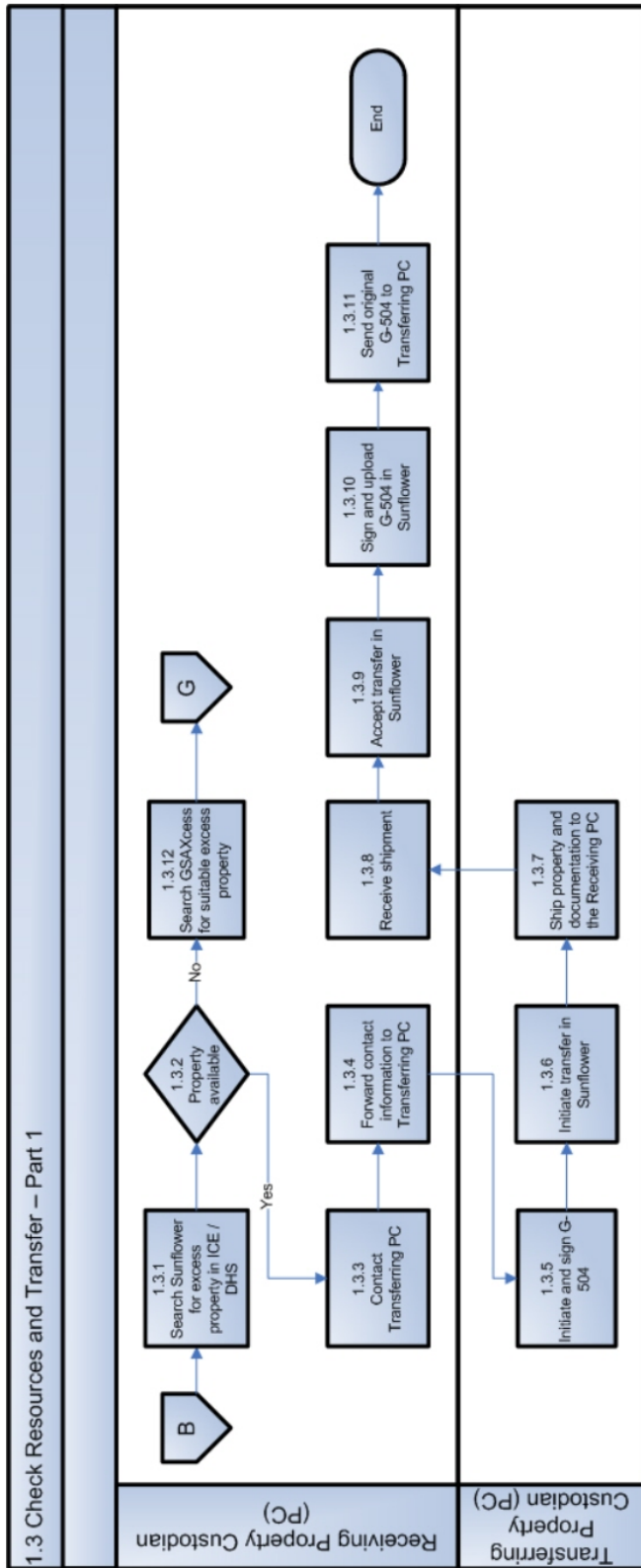


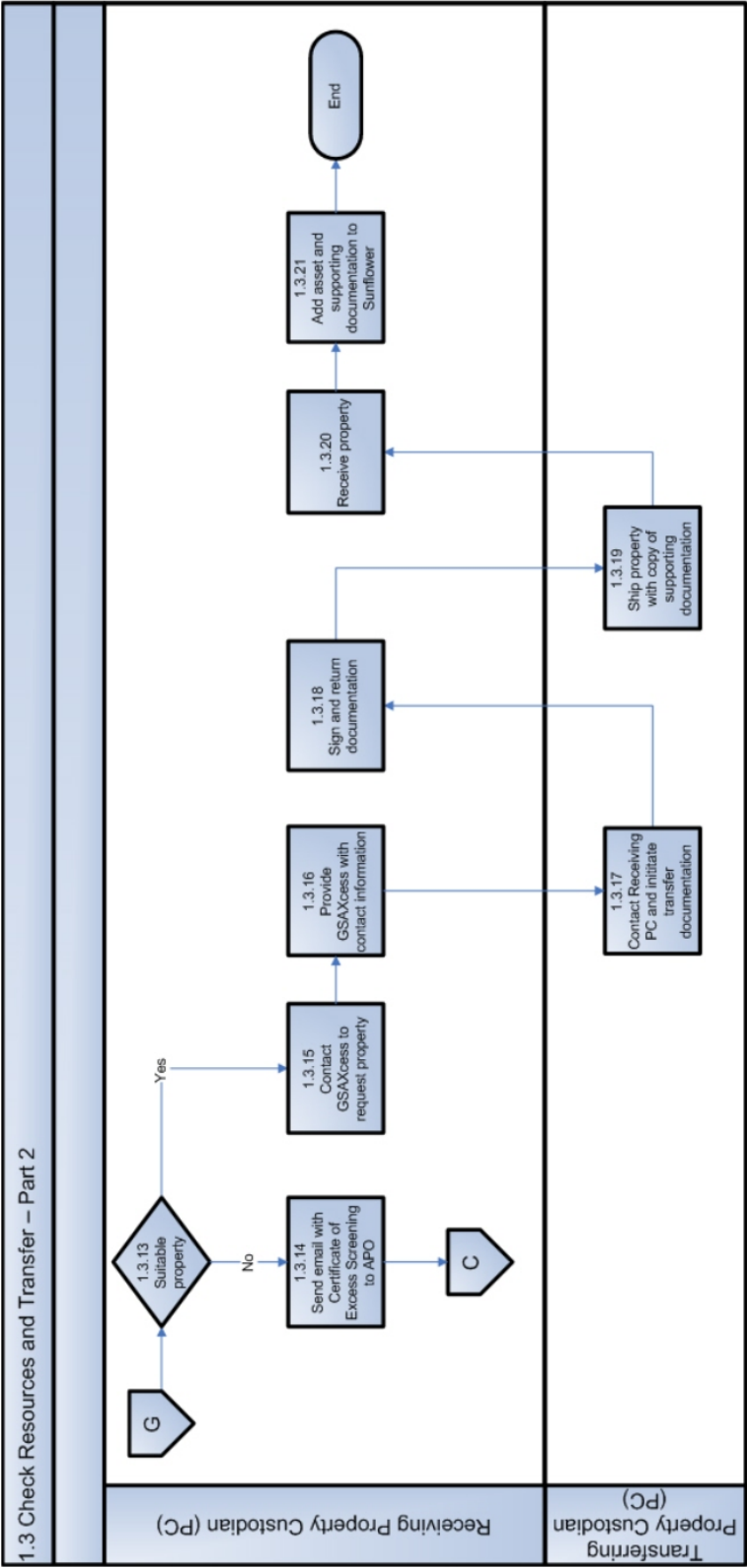


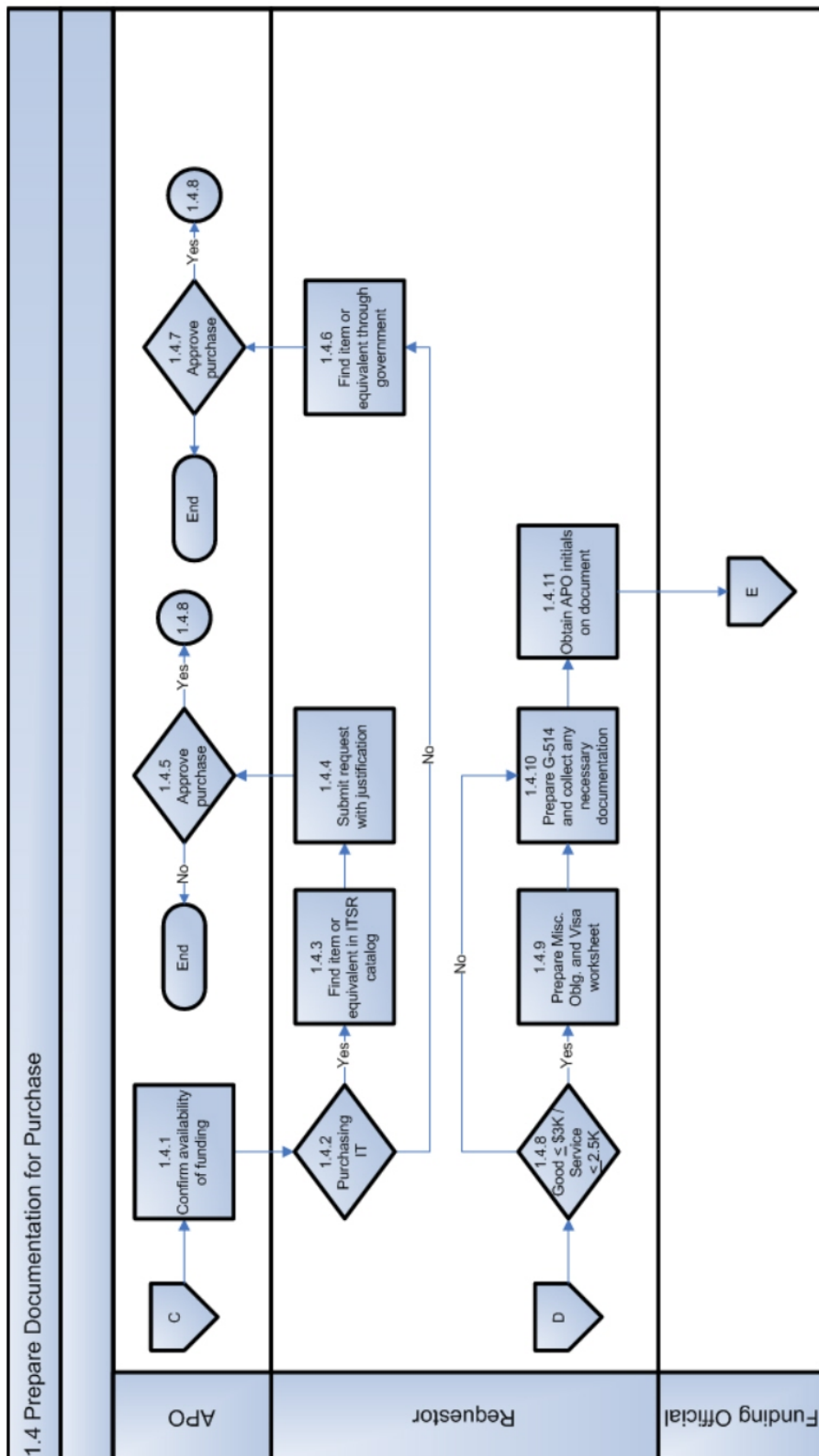


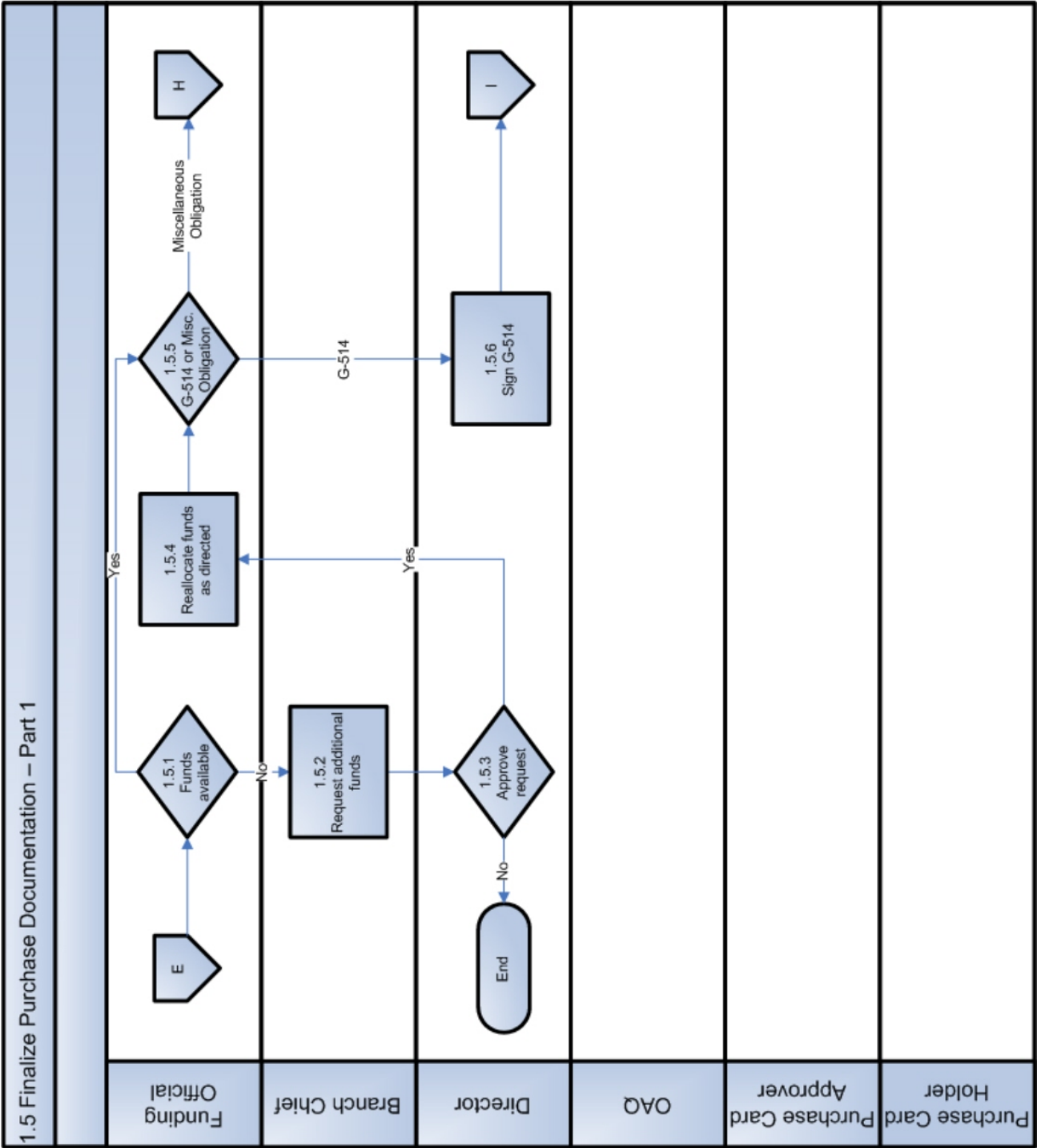


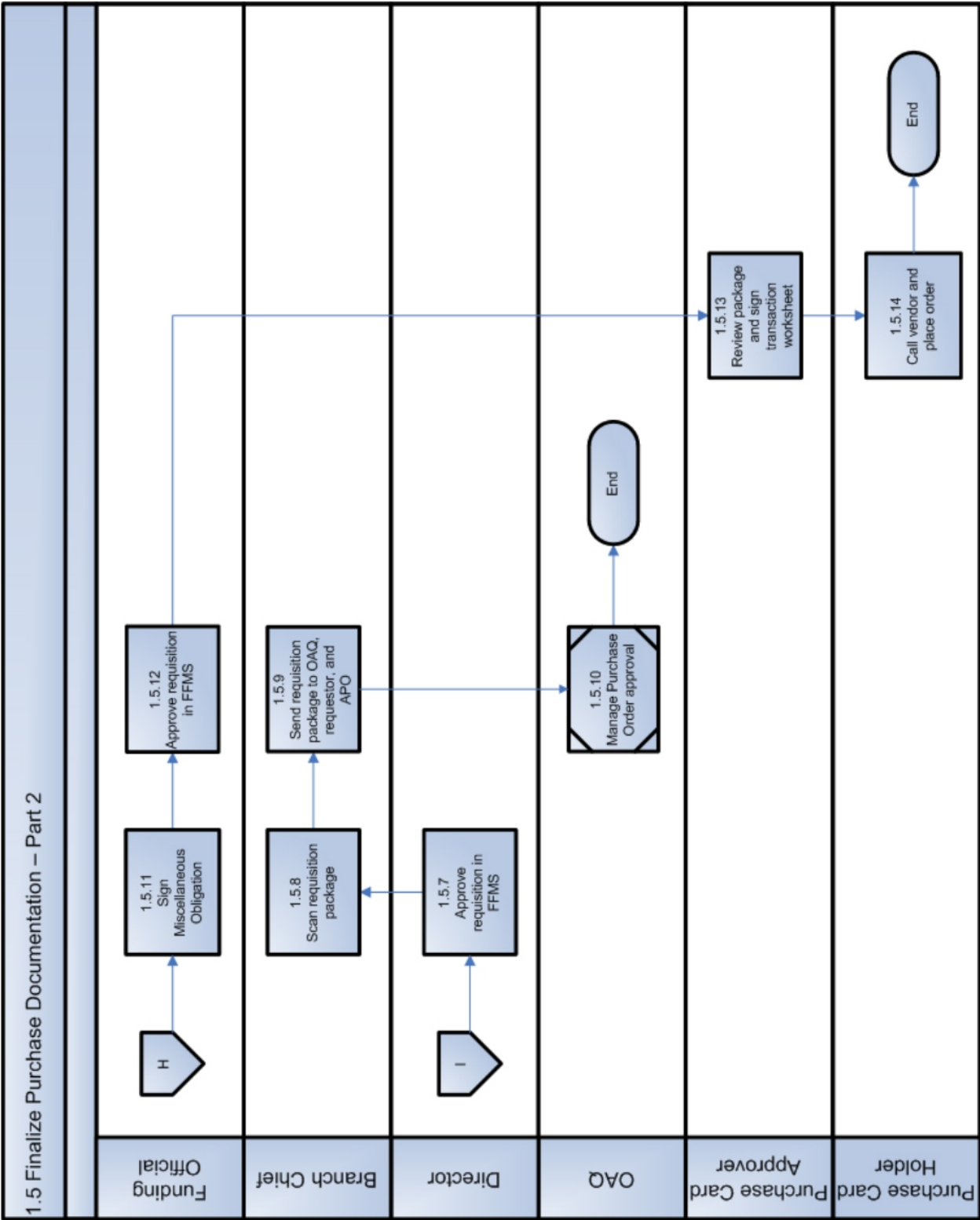


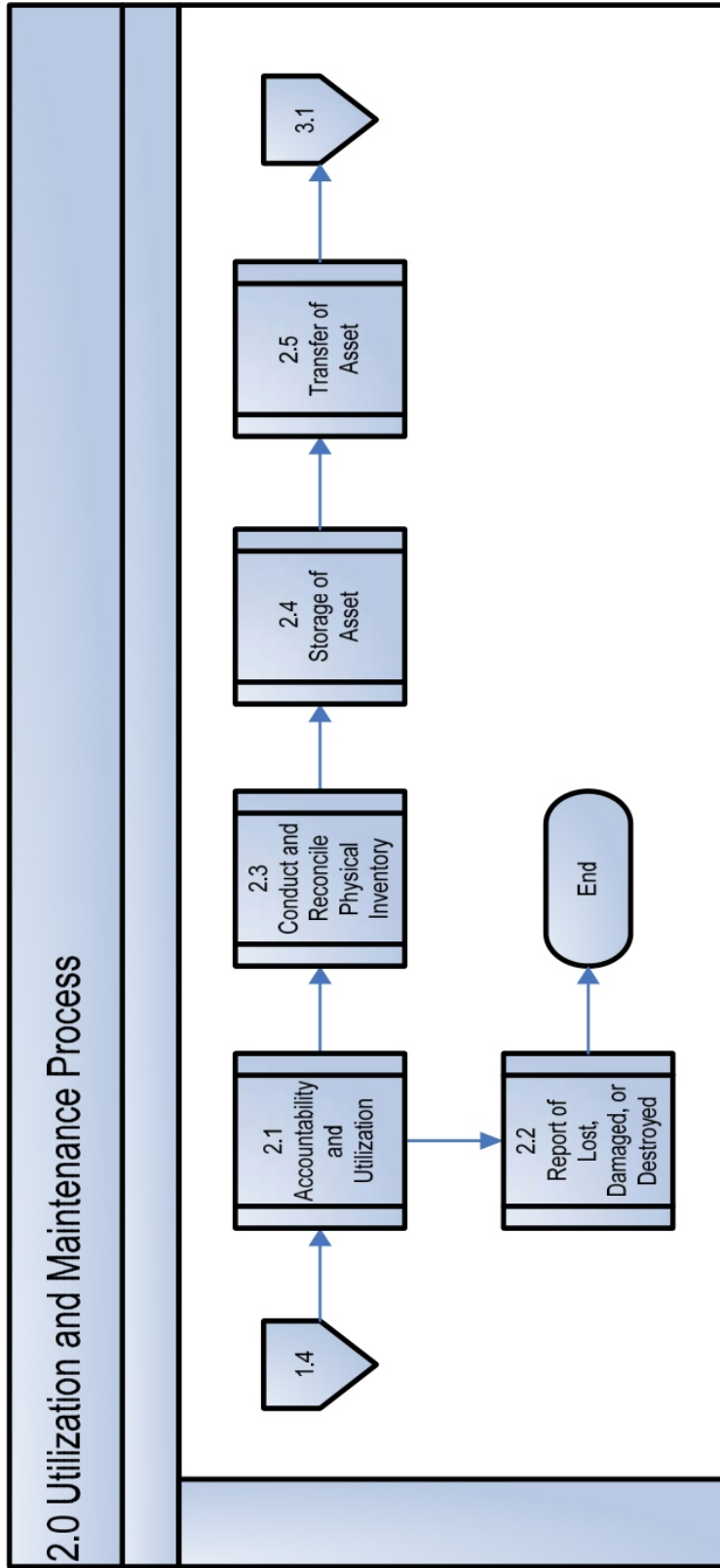


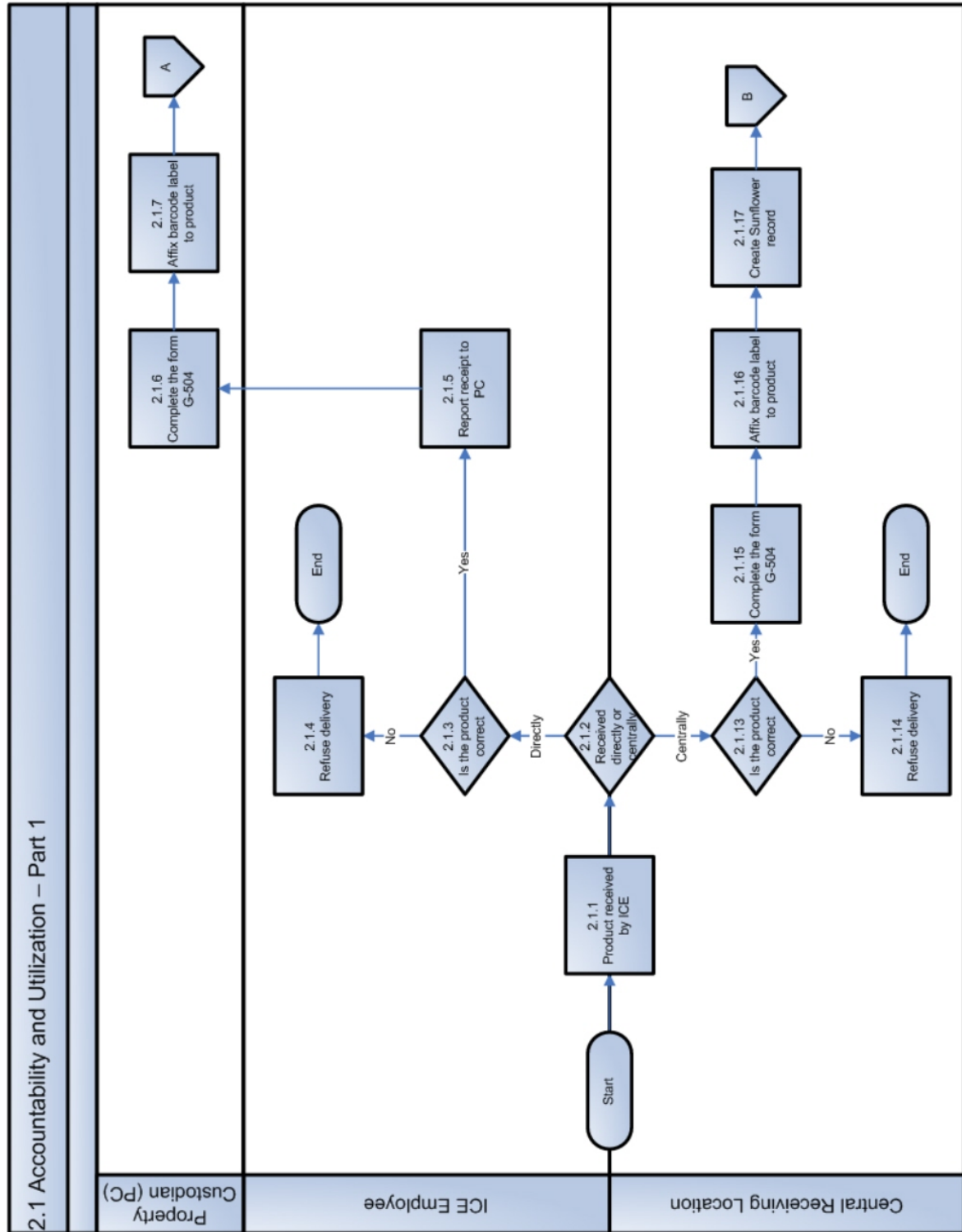


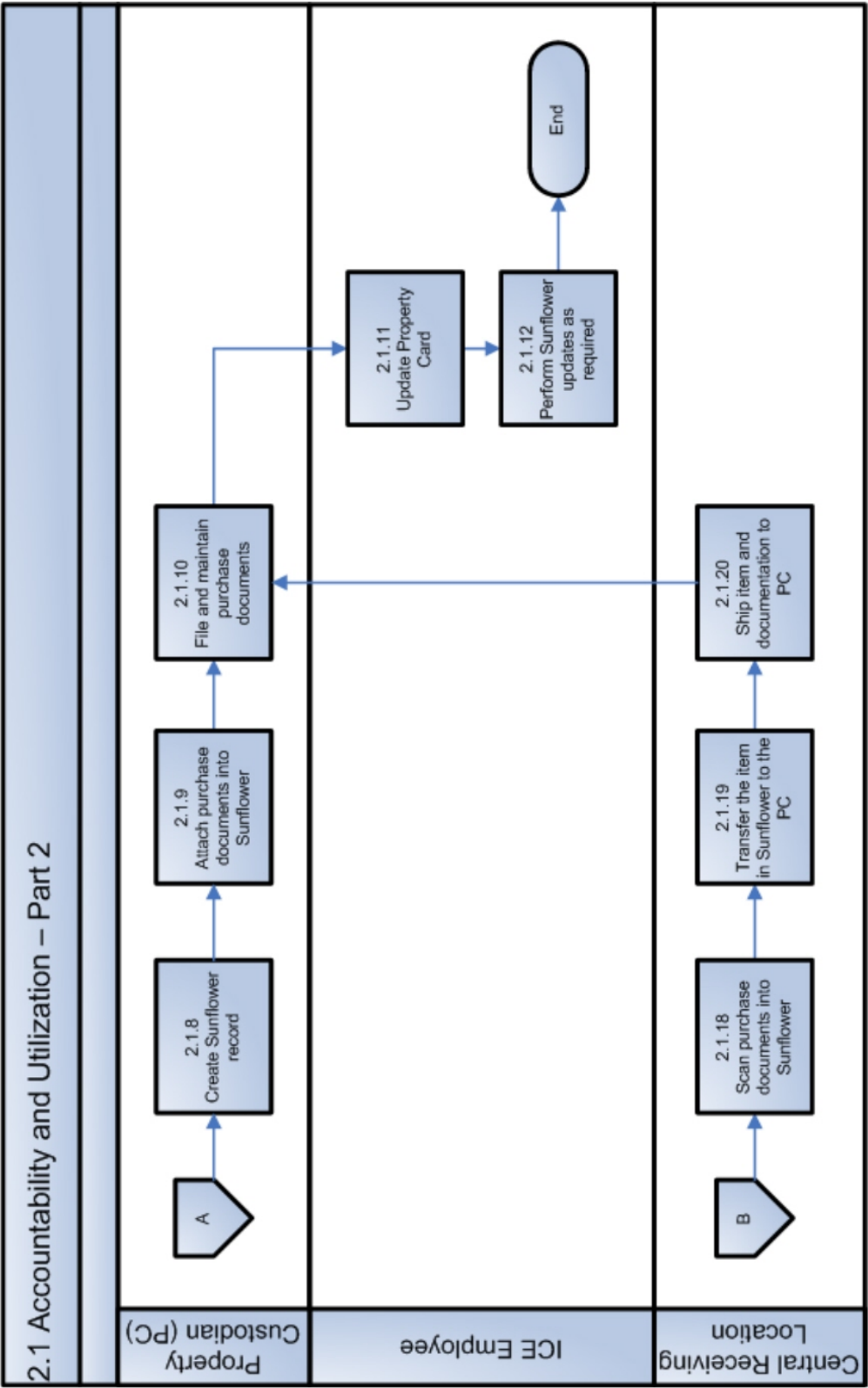


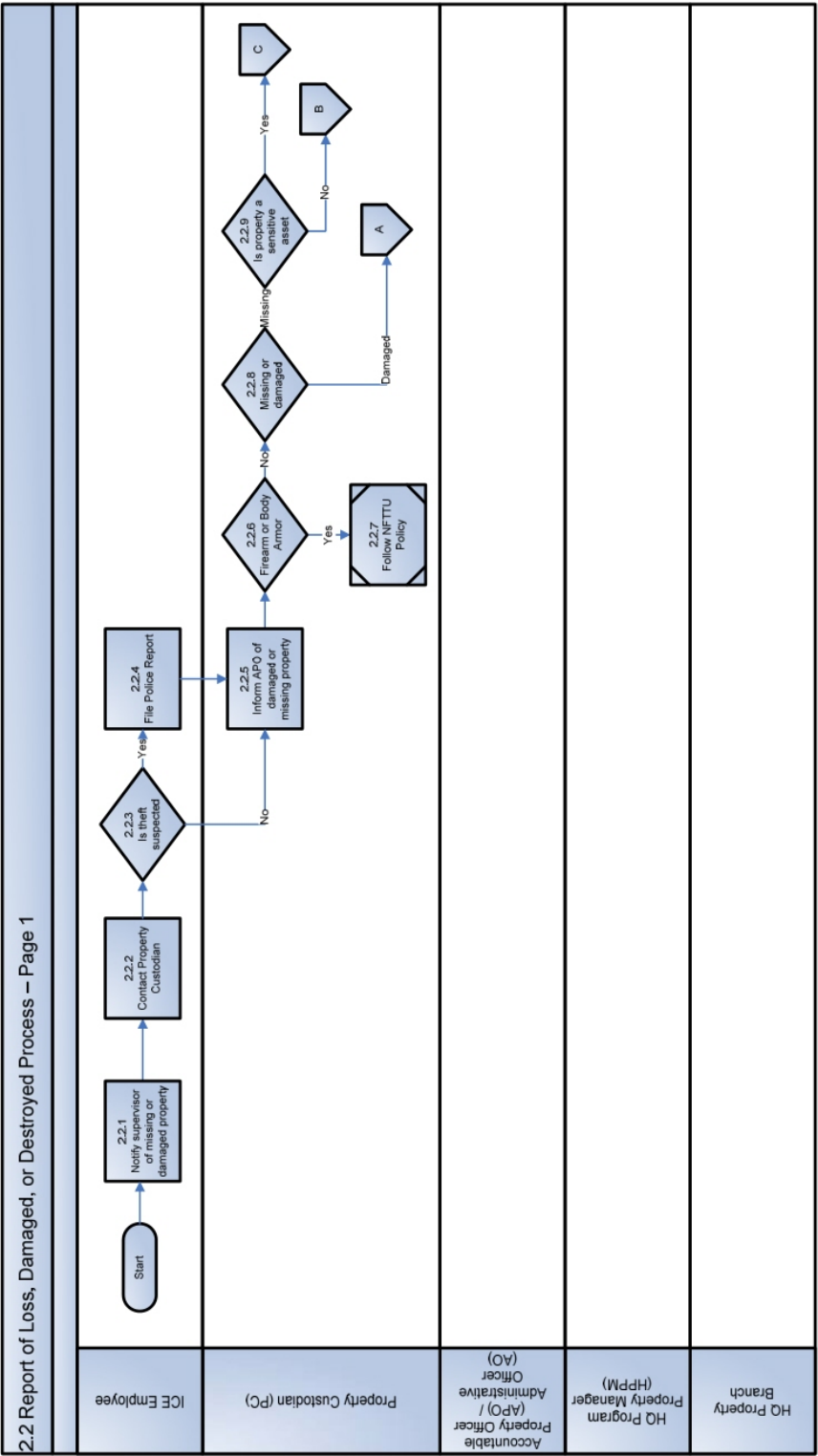


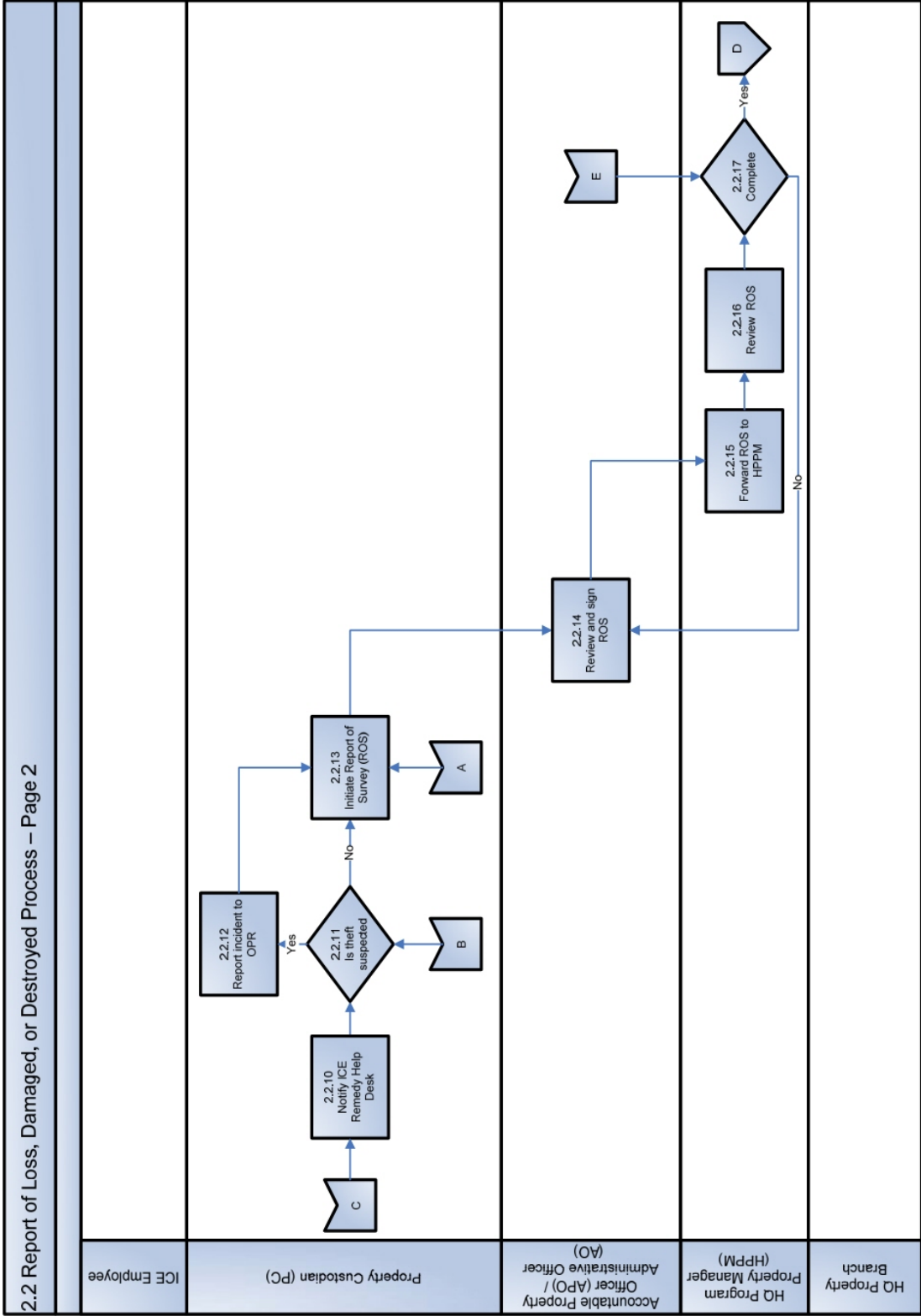


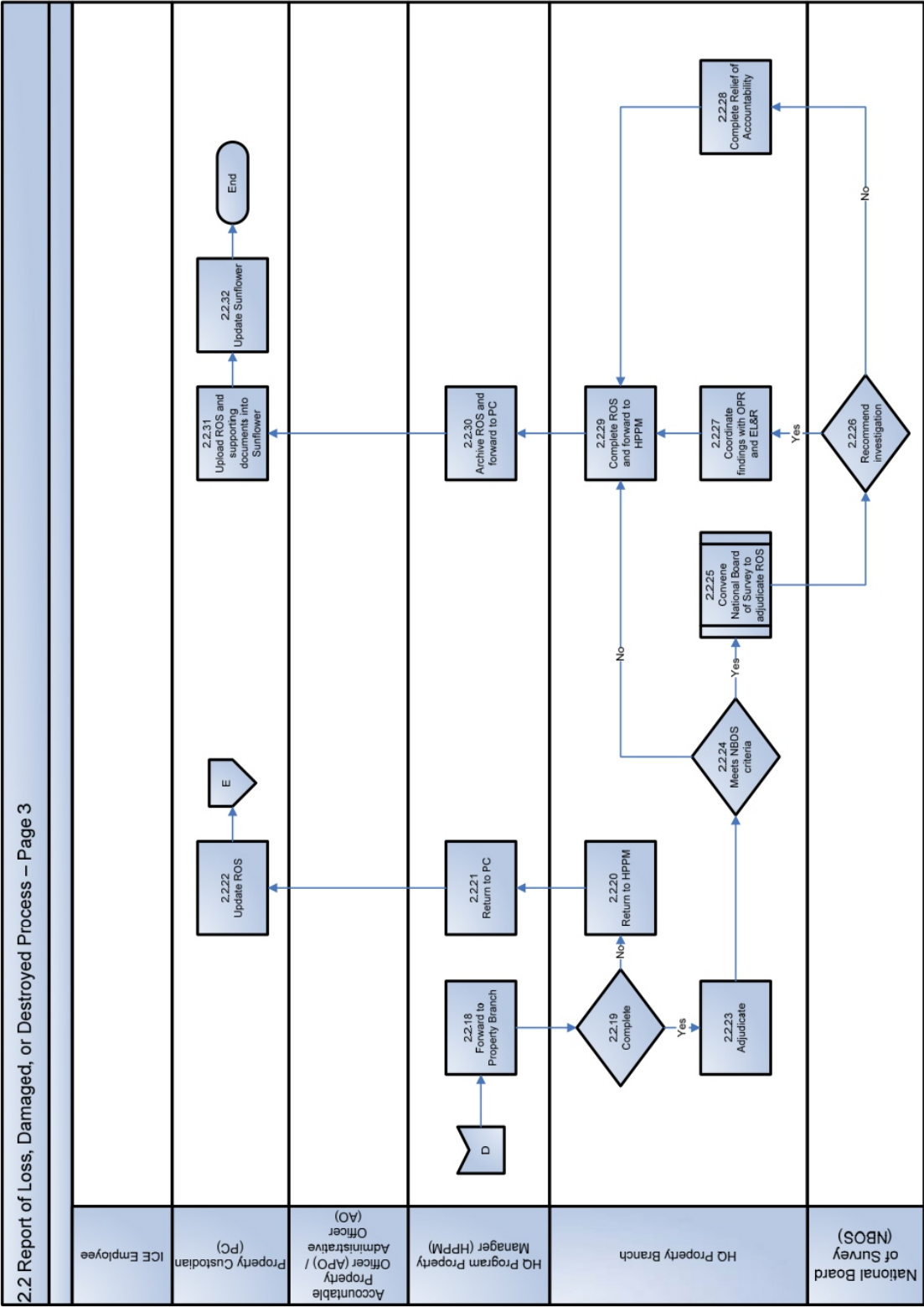


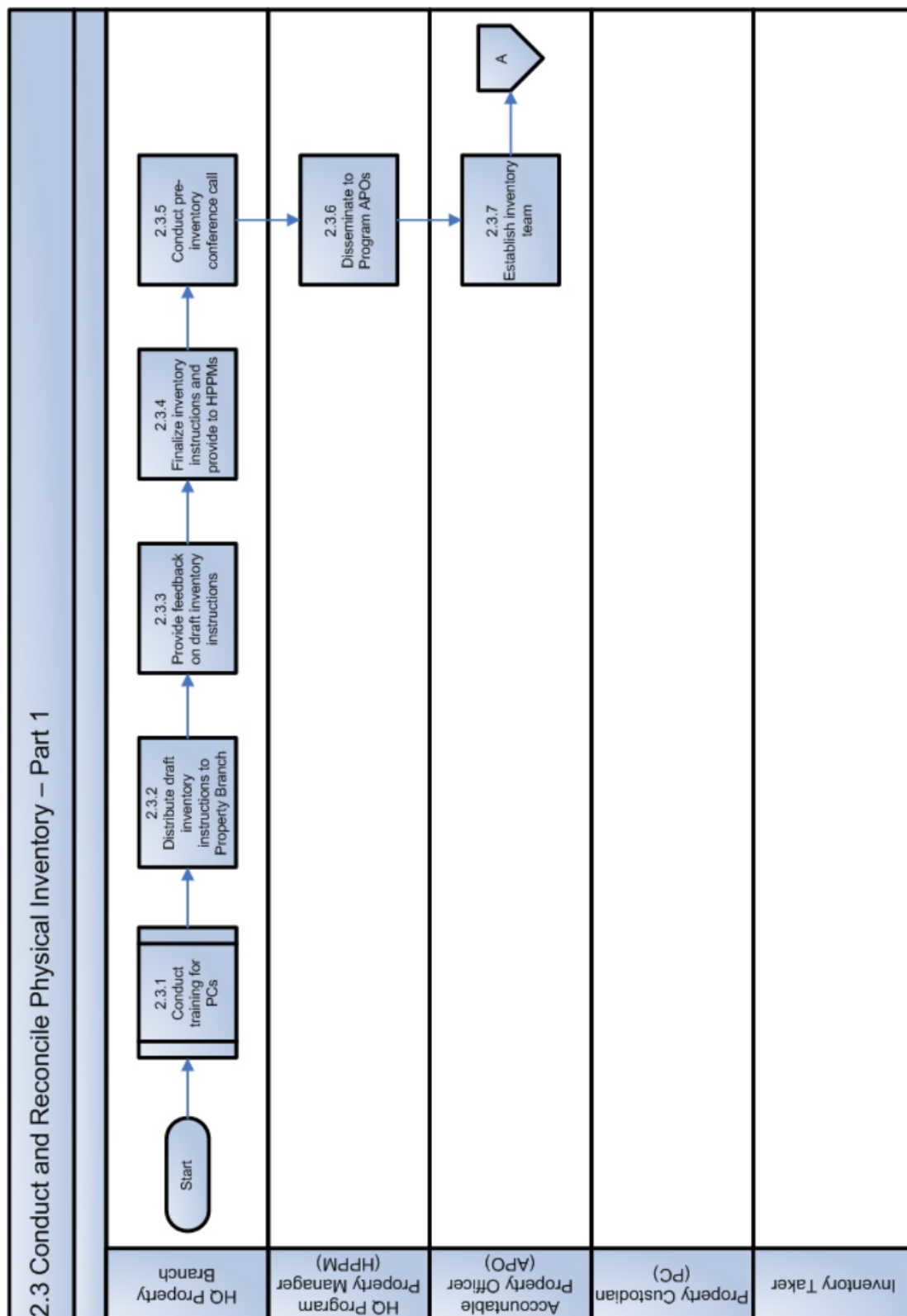


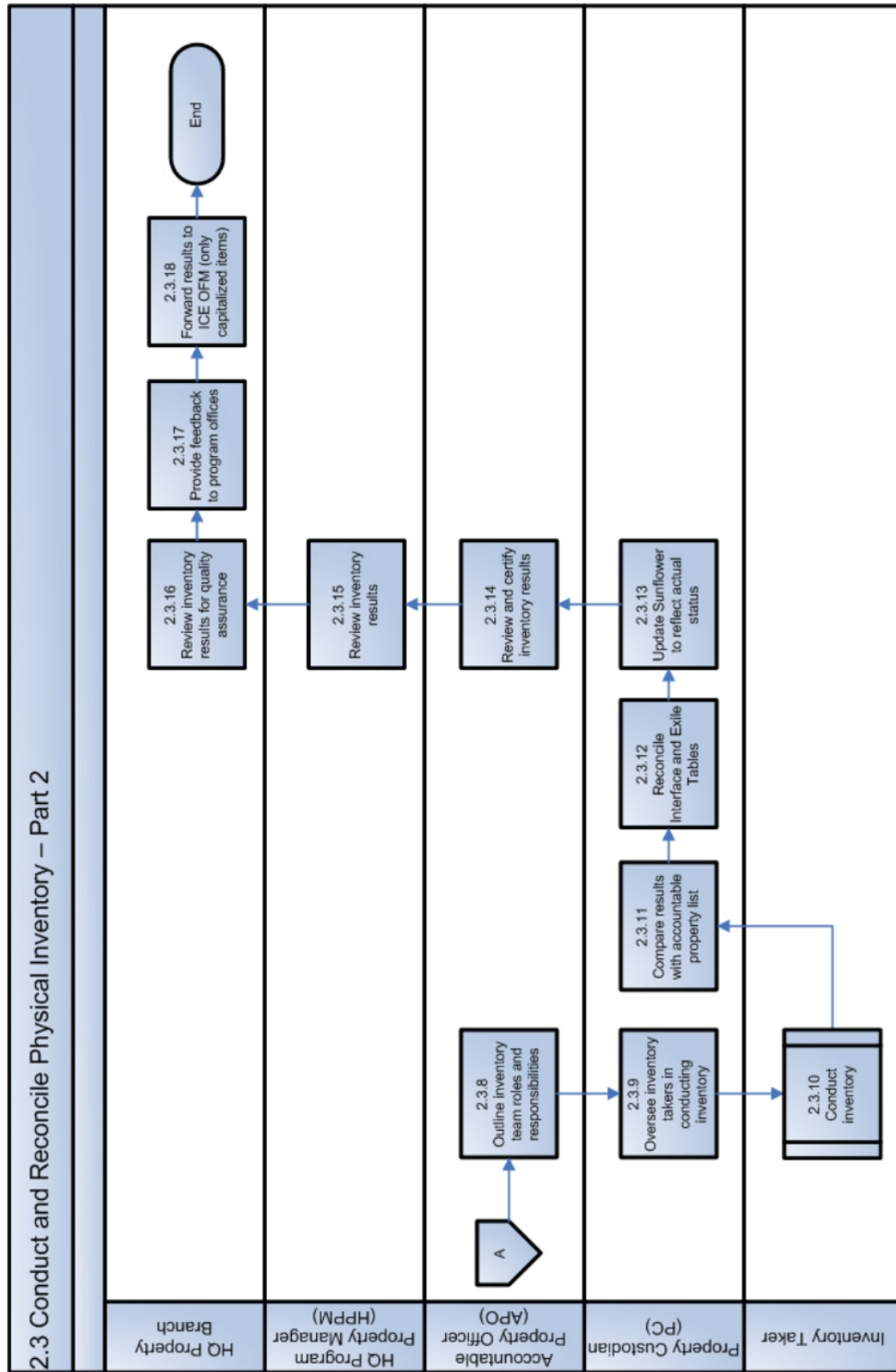


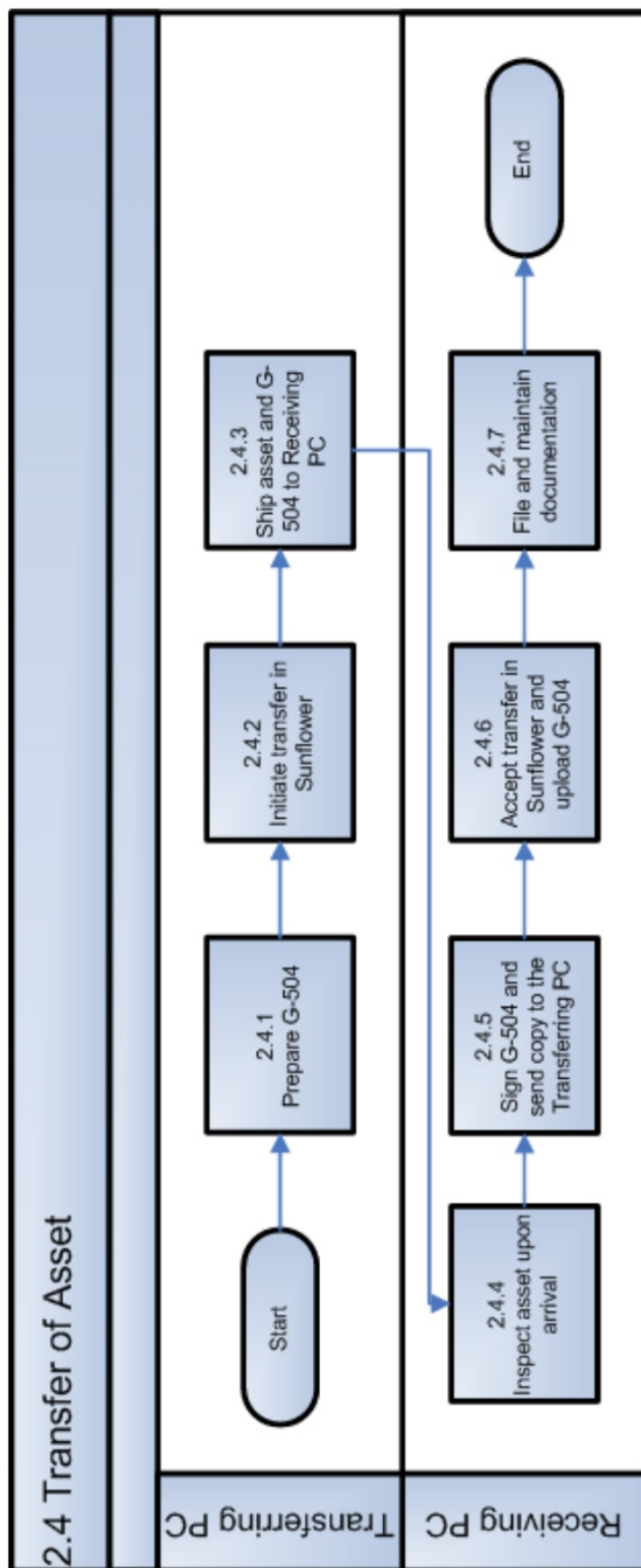


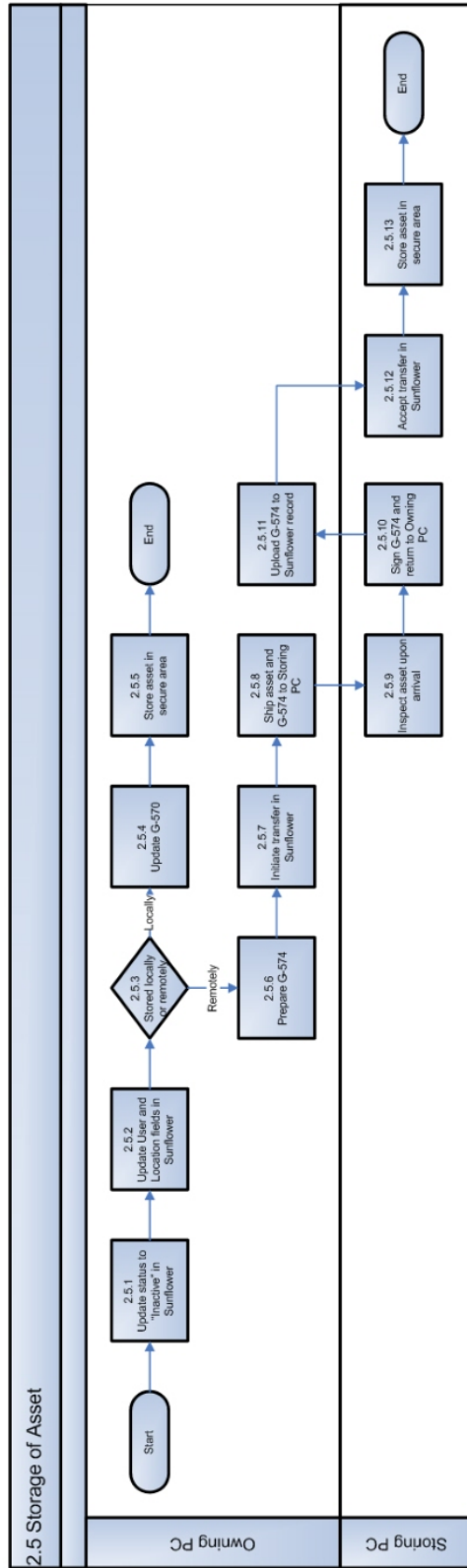


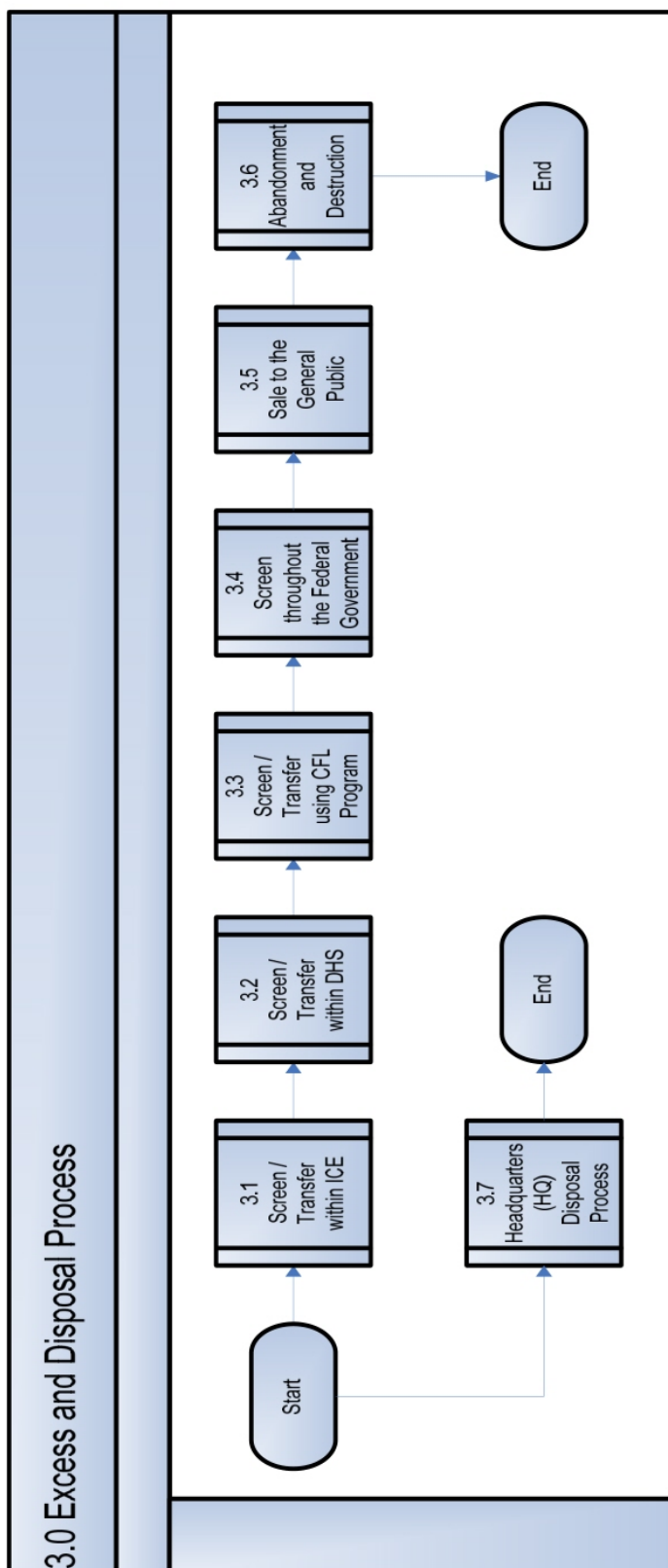


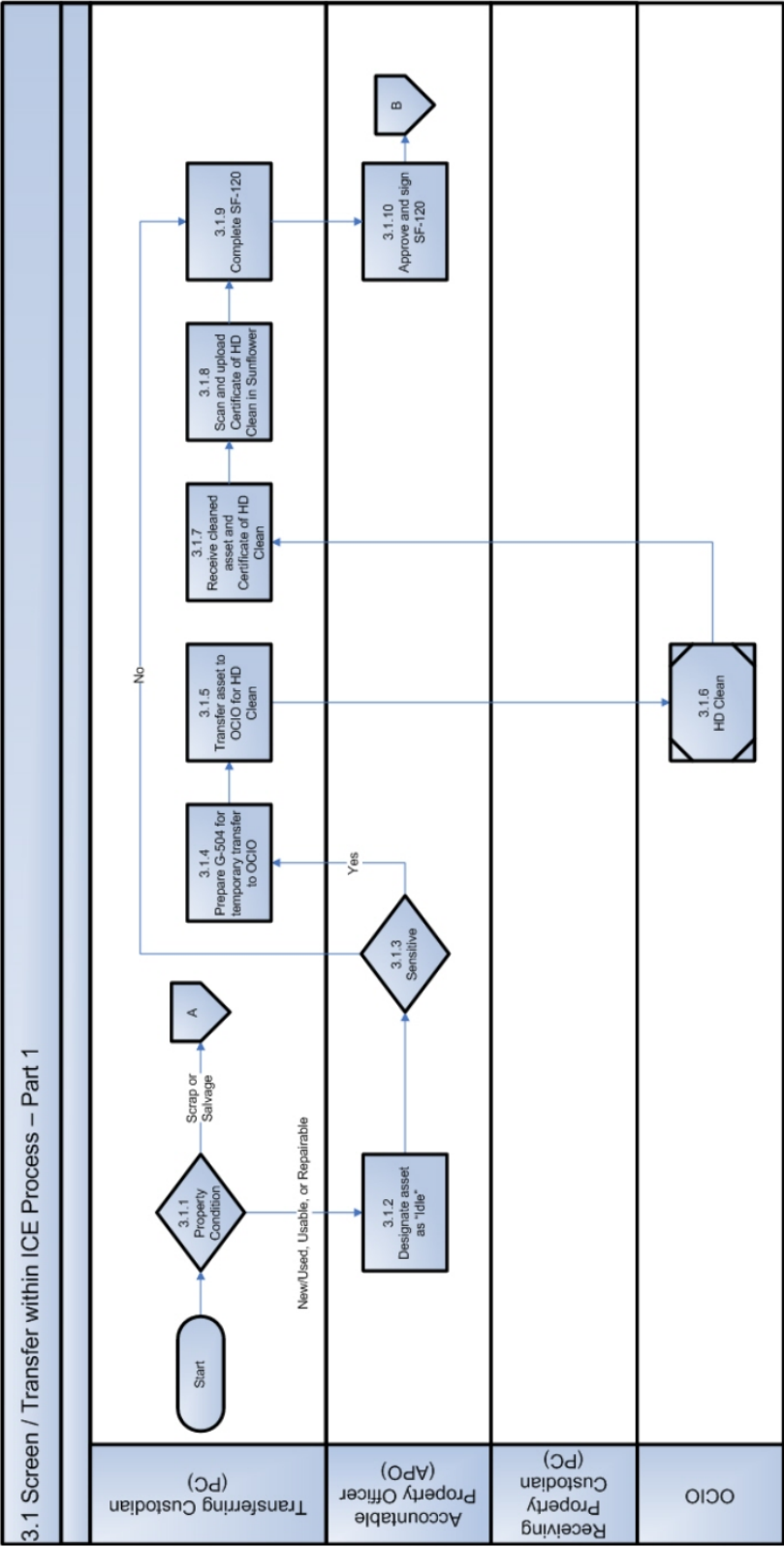


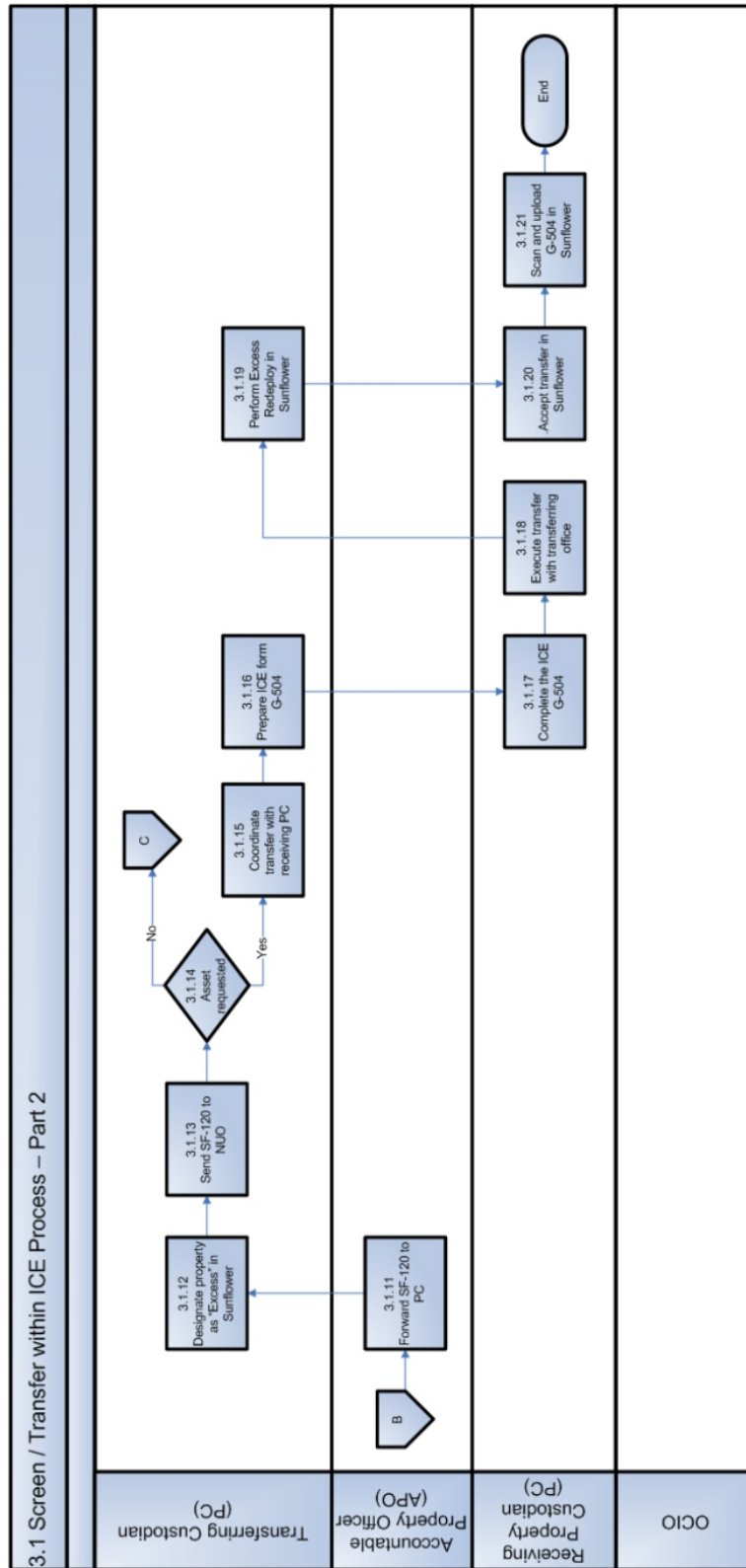


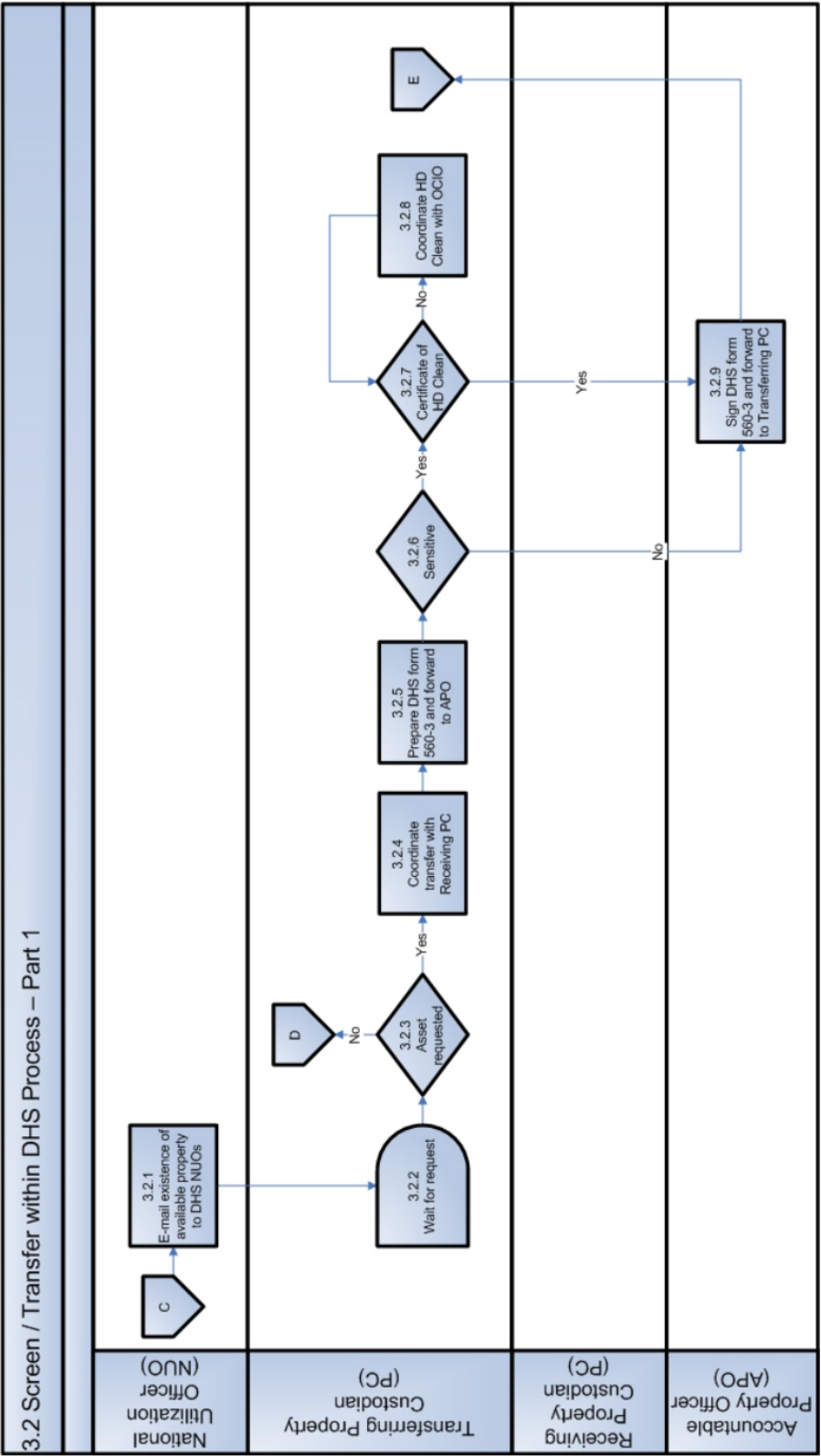


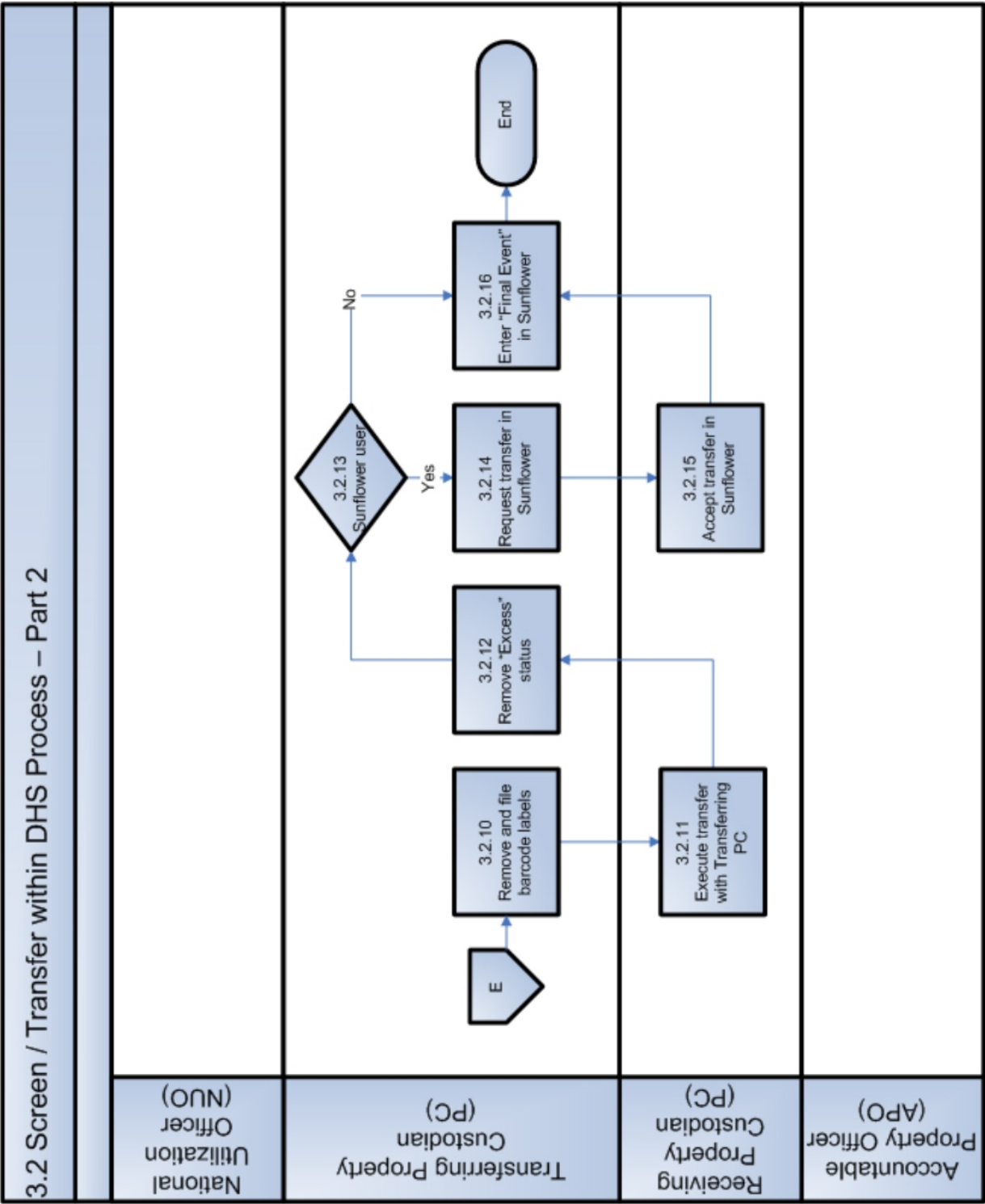


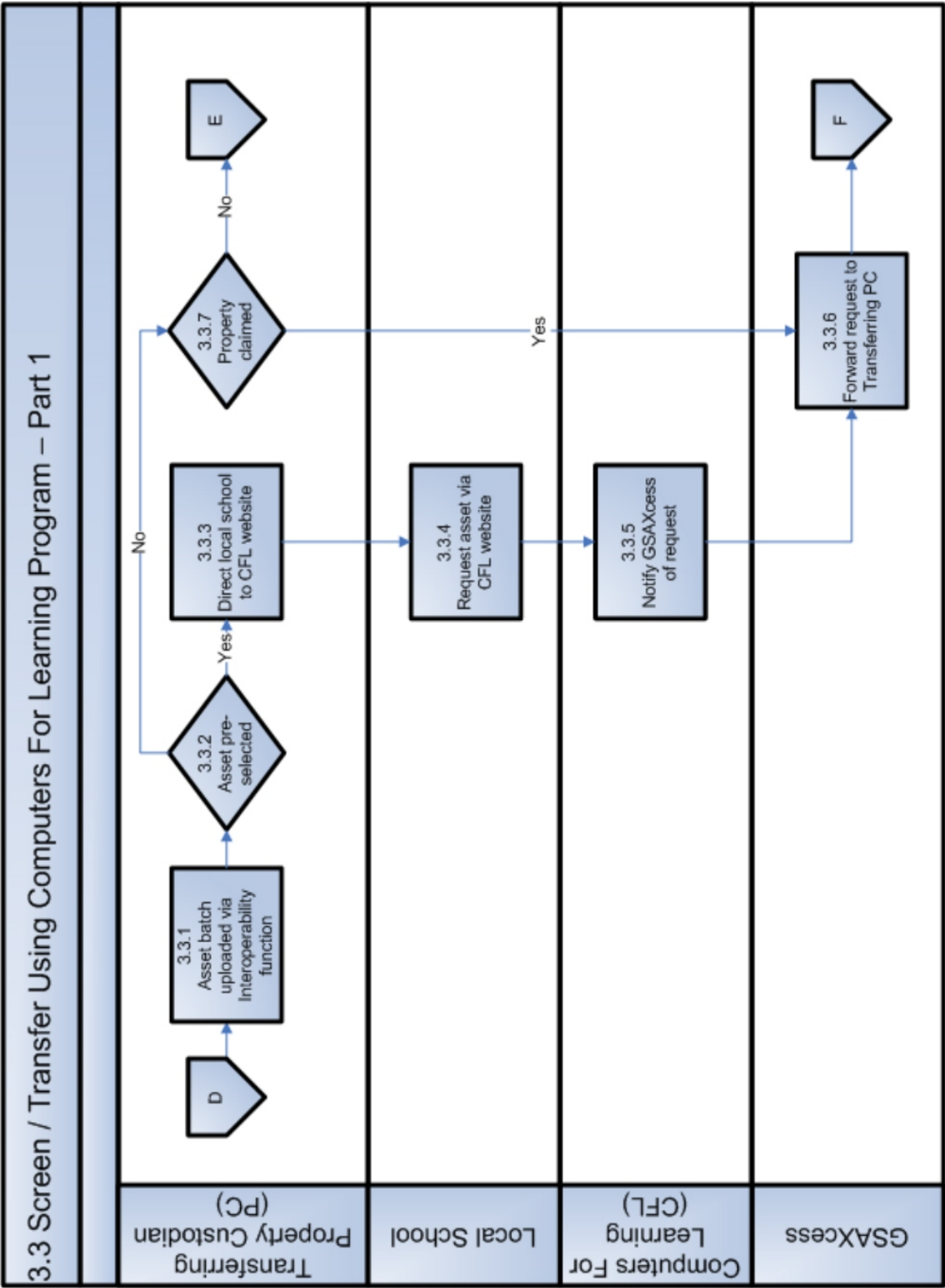


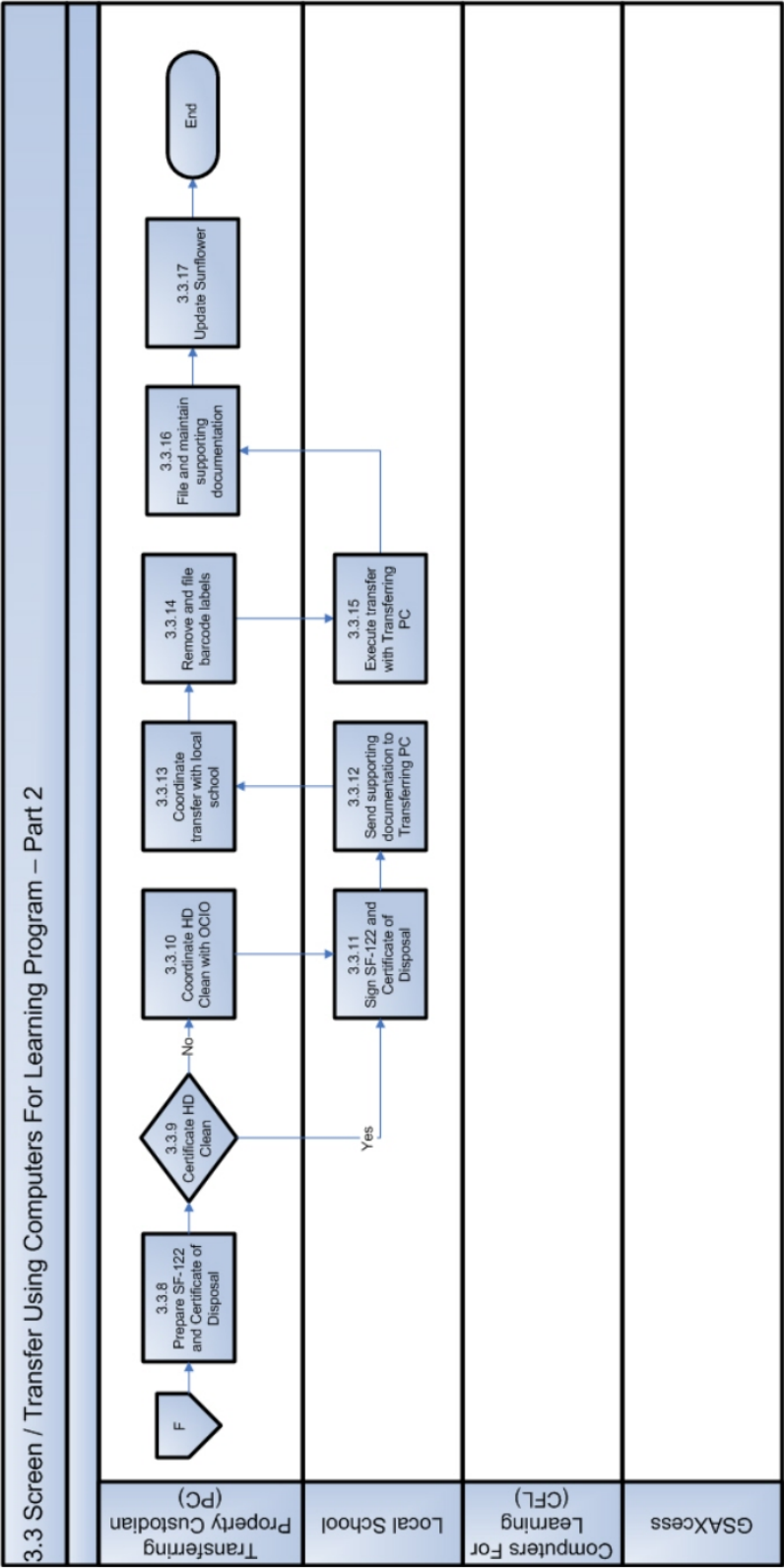


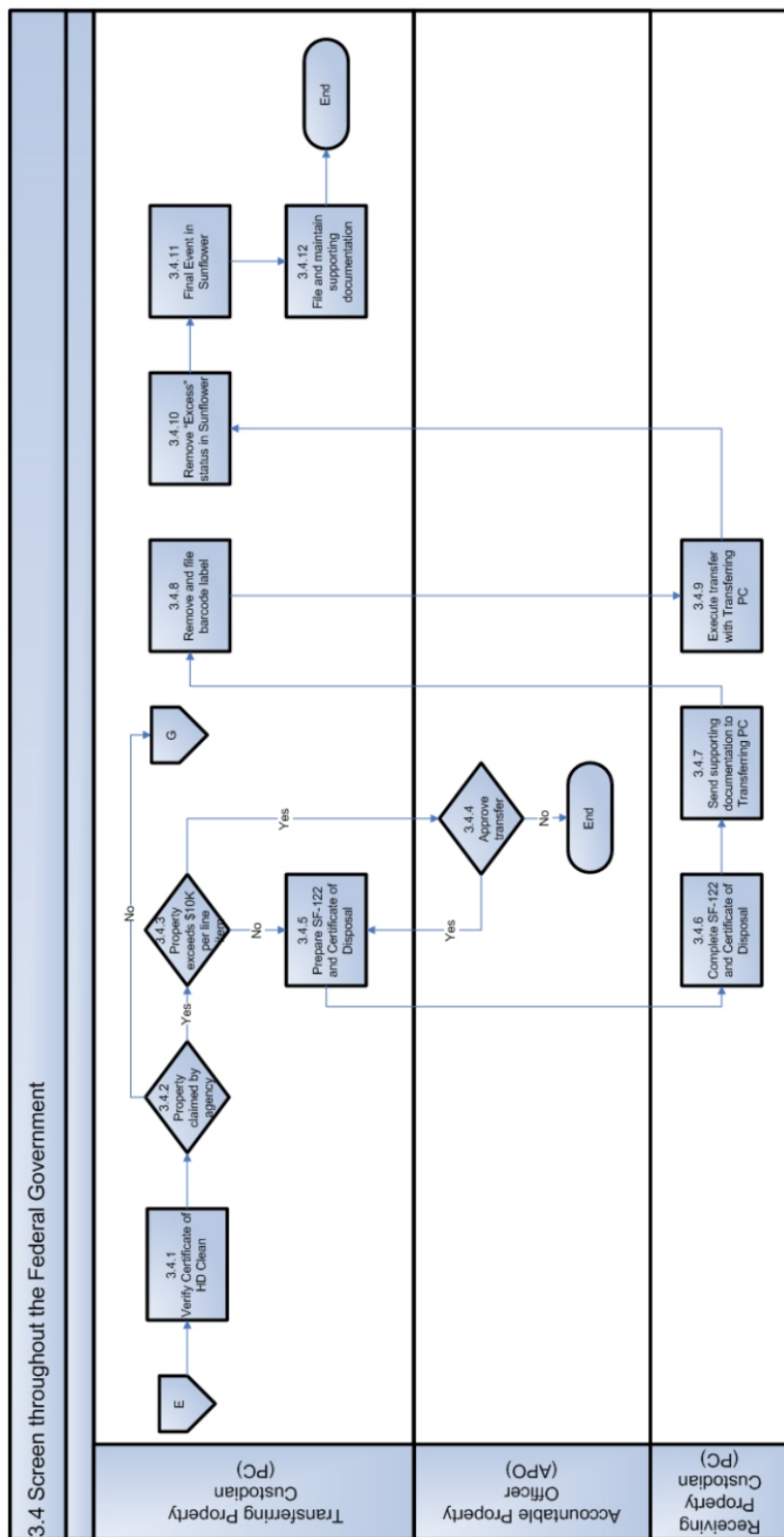


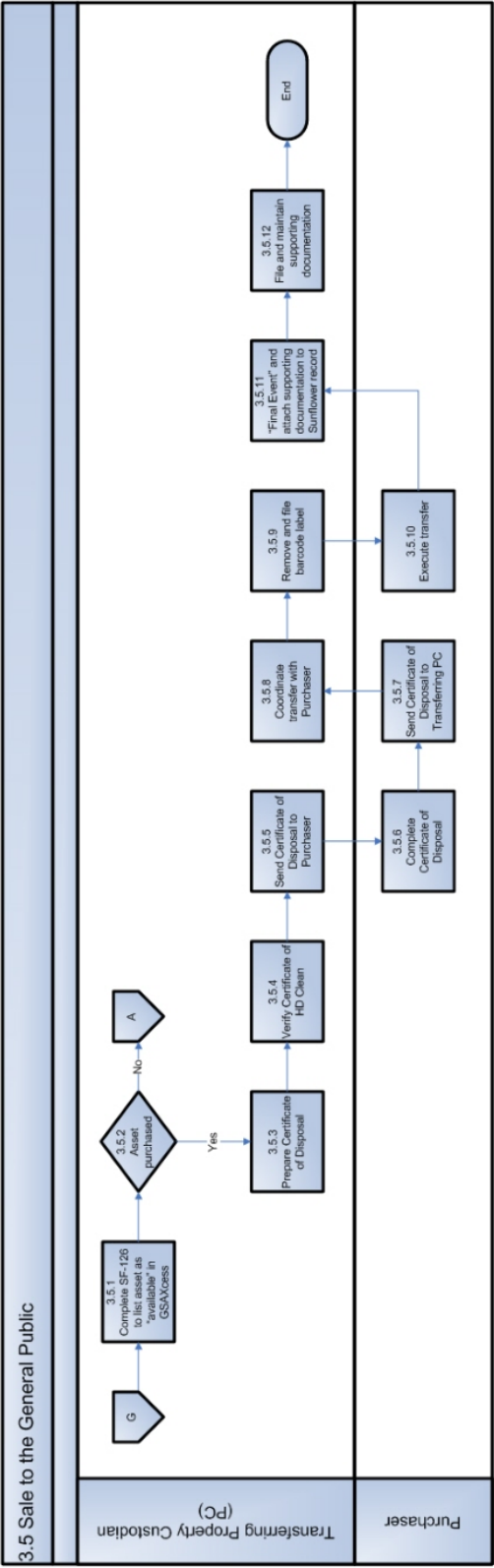


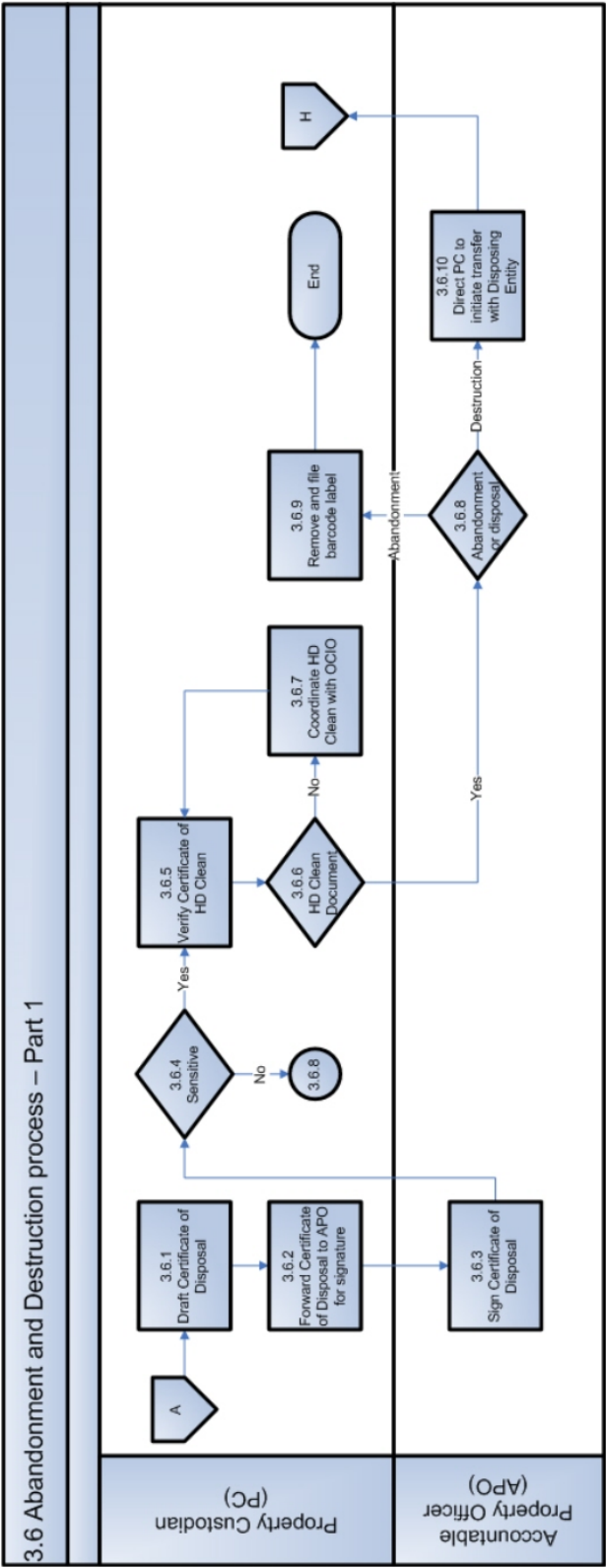


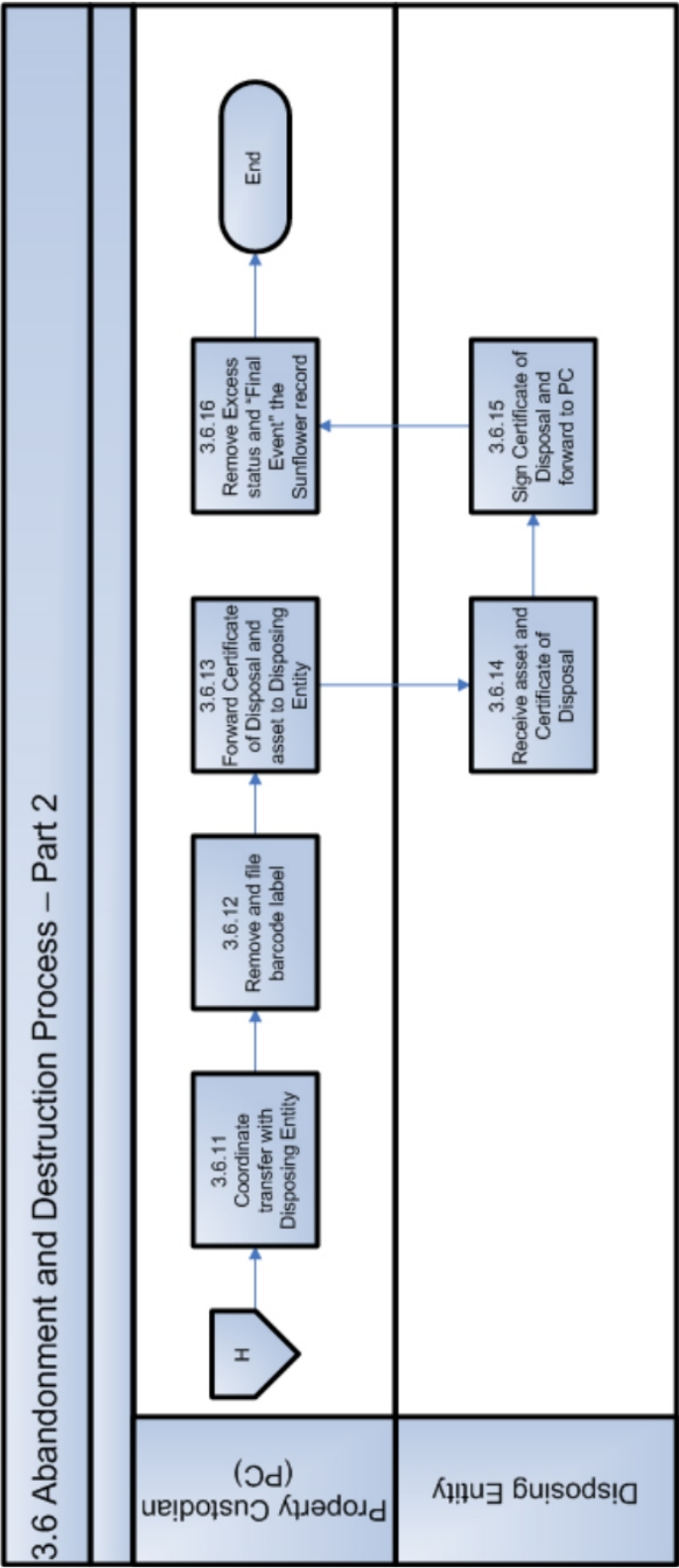


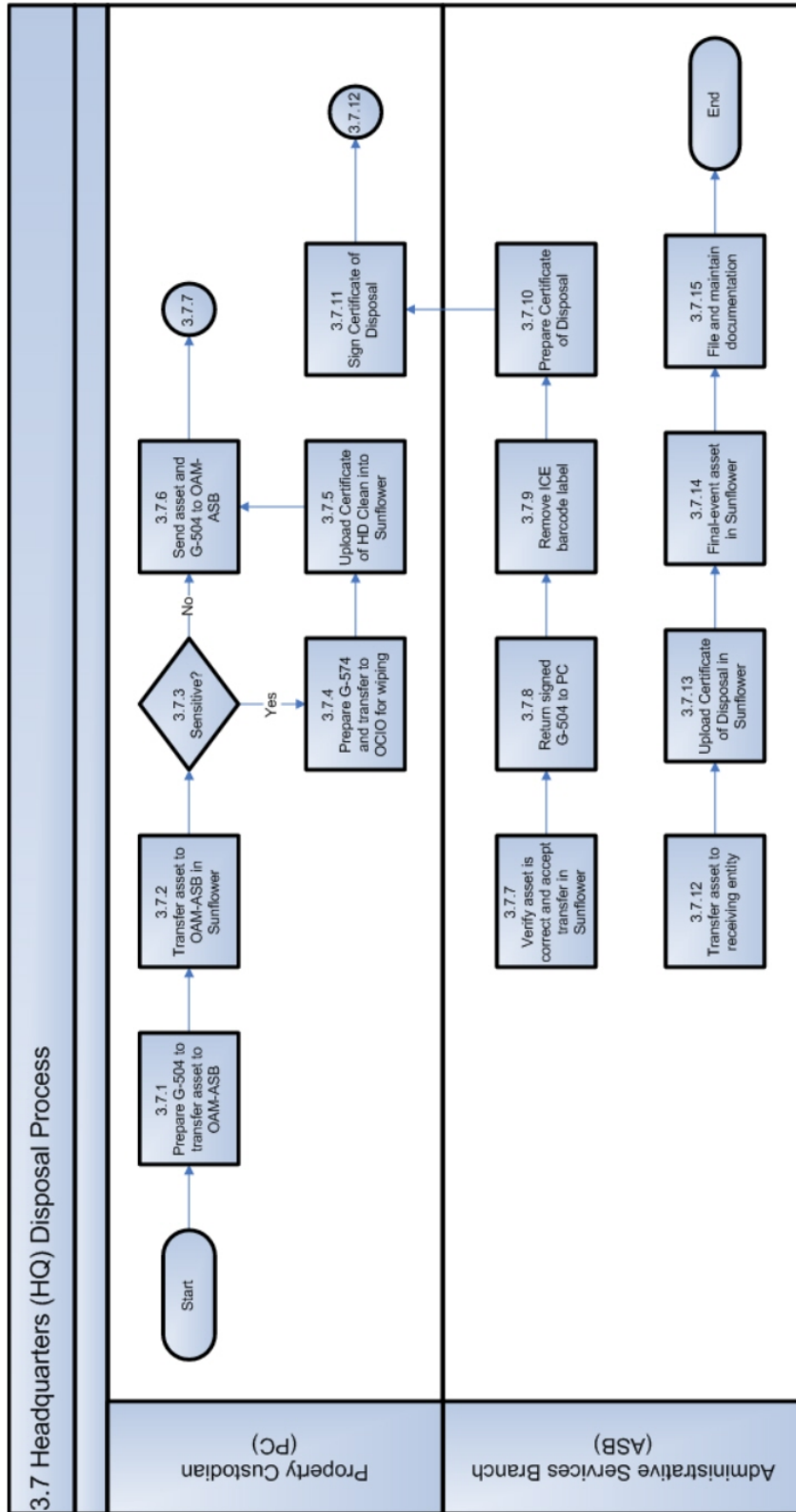












Section B

SECTION B: SUPPLIES OR SERVICES AND PRICES/COSTS

B.1 GENERAL

The Contractor shall provide all management, supervision, labor, and materials necessary to perform the services identified in the Performance Work Statement, including the purchase of detention bed at firm-fixed prices, on an Indefinite Delivery – Indefinite Quantity basis.

B.2 CONTRACT PRICING

Please see Section B of SF1449 above.

B.3 MINIMUM AND MAXIMUM QUANTITIES

In accordance with FAR 16.504(a)(4)(ii), the minimum and maximum quantity the Government will acquire under this contract is as follows:

Minimum: (b) (3) (A), (b) (4) during the period of performance of the IDIQ.

Maximum: The maximum of this IDIQ contract will be the calculated total value of the IDIQ including the base year and all options. This amount is (b) (3) (A), (b) (4)

B.4 FUNDING

Funds for the services ordered will be obligated, at the task order level, as such services are ordered, and excess funds de-obligated at the task order level, by modification to the task order contracts unilaterally by the Government.

SECTION C:
DESCRIPTION/SPECIFICATIONS/PERFORMANCE WORK STATEMENT

U.S. Department of Homeland Security
Immigration and Customs Enforcement



Performance Work Statement
Detention Services
(Texas-Wide RFP)

**See Attached PWS – Addendum A
And PWS Addendum – Requirement A – Addendum B**

Section D

**SECTION D:
PACKAGING & MARKING**

[THIS SECTION IS INTENTIONALLY LEFT BLANK]

[END OF SECTION D]

Section E

SECTION E: INSPECTION AND ACCEPTANCE

E.1 CLAUSES INCORPORATED BY REFERENCE (FAR 52.252-2) (FEB 1998)

This contract incorporates the following clauses by reference with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text can be accessed electronically at this internet address:

<http://acquisition.gov/far/index.html>.

Clause Number	Clause Title	Date
52.246-4	Inspection of Services – Fixed Price	Aug 1996
52.246-6	Inspection of Services – Time and Material and Labor Hour	May 2001

E.2 INSPECTION REQUIREMENTS

Review of Deliverables ---

- a. The Contracting Officer or Contracting Officer's Representative will provide written acceptance, comments and/or change requests, if any, within thirty (30) business days from receipt by the Government of the initial deliverable.
- b. Upon receipt of the Government comments, the Contractor shall have fifteen (15) business days to incorporate the Government's comments and/or change requests and to resubmit the deliverable in its final form.
- c. If written acceptance, comments and/or change requests are not issued by the Government within thirty (30) calendar days of submission, the draft deliverable shall be deemed acceptable as written and the Contractor may proceed with the submission of the final deliverable product. The Contractor shall provide all deliverables to the COR in Microsoft Excel, PowerPoint or Word format.

E.3 DELIVERABLES CHART

#	Deliverable	Due Date
1	Quality Control Plan	With Proposal Submission; Updated as Needed

Section E

2	Plans, Policy and Procedures Manual	Plan and Policy: as required with Proposal Submission; Procedures Manual: 5 days after award
3	Standard Operating Procedures	Within 30 calendar days of award of contract
4	Post Orders	Within 30 calendar days of award of contract, annually and as requested by the COR.
5	Communication Plan	With Proposal Submission; Updated as Needed
6	Resumes of Key Personnel	Submitted within 5 days after award. For all new candidates, prior to Entry on Duty (EOD)
7	Organizational Chart	With Proposal Submission and after that, anytime as requested.
8	Staffing Plan	With Proposal Submission and after that anytime as requested by the COR.
9	Documentation of employee receipt of ICE Operations Policy/Procedure Manual	As requested by COR
10	Contractor employee certification for standards of conduct	As requested by COR
11	Contractor employee violation of standards of conduct and disciplinary action	Reported immediately* to COR
12	Notification of change in employee's health status	Notification immediately to COR (immediate verbal report, with written follow-up)

Section E

13	Employee termination, transfer, suspension, personnel action relating to disqualifying information or incidents of delinquency	Notification immediately to COR (immediate verbal report, with written follow-up)
14	Report of any on contract employee misconduct	Notification immediately to COR (immediate verbal report, with written follow-up)
15	e-QIP Security Process	Prior to Entry on Duty (EOD)
16	Physical Force Incident Reports	Reported to COR immediately (immediate verbal report, with written report within two (2) hours of incident)
17	Report of escapes	Reported to COR immediately (immediate verbal report, with written report within two (2) hours of incident)
18	Physical harm or threat to safety, health or welfare	Reported to COR immediately (immediate verbal report, with written report within 24 hours of incident)
19	Drug Test Results	Upon EOD and as requested by COR, or reported immediately to COR upon found violation
20	Emergency Call Back Roster	Quarterly or as needed
21	Training Plan, with Curriculum	Within 30 calendar days of award of contract; Updated as Needed
22	Quarterly Training Forecast	Quarterly
23	Training certification and reports for formal and on the job training (including Supervisors and refresher)	As requested by COR
24	Daily Time Sheet	As requested by COR

Section E

25	Emergency Action Plan to include Auxiliary Power procedures	Within 30 calendar days of award of contract; Updated as Needed
26	Sexual Assault & Suicide Prevention Program	No later than the post award conference
27	Firearms Training Certificates	Annually
28	Employee Weapon Permit	To COR 3 days prior to EOD, and then after as requested by COR
29	Notification of employee criminal activity	Reported immediately to COR and appropriate law enforcement agency.
30	Officer Testing Questions and Results	Post award, as needed by the COR
31	Key, Tool Cabinet Inventory Class A and Class B Log	At the beginning of day and end of each shift
32	Equipment Inventory	Within 30 calendar days after award of contract, then annually or as requested by COR
33	Intervention Equipment Inventory	Within 30 calendar days after award of contract, then annually or as requested by COR
34	Regular Tool Control Log	Monthly
35	Detainee Volunteer Work Screening Form (Request Form)	As required
36	Detainee Volunteer Work Program Training Form	As required
37	ACA Accreditation	Within 18 months of contract award

Section E

38	Proposed daily transportation routes	Within 30 calendar days of contract award
39	Safety Devices/Equipment Training Plan	Quarterly
40	Chemical Perpetual Inventory Sheet	As requested by COR
41	Compliance and Independent Audit Report	Annually
42	Key Indicators Report	Monthly, by 5 th of each month for previous month's data
43	General Supply/Inventory Plan	Within 30 calendar days after award of contract, then annually or as requested by COR
44	Commissary Inventory List	As requested by COR
45	Statement of Detainee Funds Accounts	As requested by COR
46	IT Security Plan	Within 30 calendar days after award of contract
47	Finalized List of Approved Food Vendors	Within 30 calendar days after award of contract and upon any changes thereafter
48	Prime Vendor/Food Service Expenditures	As requested by COR
49	Employee Meal Ticket Sales Report	As requested by COR
50	Number of Meals Served/Daily Meal Count	Quarterly or as requested by COR
51	Detainee Records	Continuous

Section E

52	Detainee Death	Reported immediately to COR (immediate verbal report, with written report within two (2) hours of incident)
53	Detainee Departure Documents	Continuous, prior to detainee departing.
54	Detainee Volunteer Food Service Worker Contingency Plan	Within 30 calendar days of award of contract and after that anytime as requested by the COR.
55	35 Day Regular Menu	Monthly
56	Physical damage to the facility documentation	Immediate verbal report to COR, with written report within five (5) days.
57	Detainee Special Needs Menu	As requested by COR
58	Daily Diet List (Medical & Religious)	As requested by COR
59	Holiday Menus	Annually
60	Emergency Food Preparation and Service Schedule	Within 30 calendar days of award of contract
61	ACA Temperature Log Report (refrigerators, freezers, dishwasher temperatures and water)	As requested by COR
62	Food Service Weekly Inspection Log	Weekly or as requested by COR
63	Food Handler Certification	Maintained for all food service employees at all times, and as requested by COR
64	Food and Non-Food Inventory	Monthly or as requested by COR

Section E

65	Maintenance Service Work Orders	As requested by COR
66	Common Fare Cost for Detainees	Quarterly, or as requested by COR
67	Authorized Detainee Worker List Weekly Schedule	Weekly, or as requested by COR
68	Detainee Volunteer Food Service Work Detail Pay List	Monthly
69	Monthly Medical Inspection Corrective Actions	Monthly
70	Certified Dietician In- Service Staff Training and Department Inspection	Quarterly, or as requested by the COR
71	Medical Clearance including TB test	For all new employees and after diagnosed with illness or communicable disease. Employees must be re-examined and medically cleared before returning to work. TB test certification annually.
72	Vehicle inventory log and interior specification for each vehicle type	Within 30 calendar days of award of contract, annually and as requested by COR
73	Menu Cycle (Revisions and Registered Dietician Recertification of all menus)	Annually
74	End of Month Food Service Cost Report, including Cost Per Meal Data	Annually
75	Firearms Control Register	As requested by COR

Section E

76	Surveillance Video	As requested by COR
77	Detainee or Contractor Employee Contraband Found Report	Immediately to COR (immediate verbal report, with written follow-up)
78	Staff Vacancy Report	To COR by 5 th of each month for previous month's data
79	Additional Reports as requested by the COR	As needed
80	Notice of facility readiness	10 days prior to the end of the Transition Period
81	Records related to performance by contractor	As requested by CO or COR at any time during the term of the contract or at termination/expiration.
82	Litigation	As requested by CO or COR at any time during the term of the contract or at/after termination/expiration.
83	Congressional Inquiry	Immediately to COR and CO (immediate verbal report, with written follow-up) to FOD, DFOD, COR, and CO
84	Press statements and/or releases	To FOD, DFOD & COR prior to release
85	Correctional Officer assignment, Names of Supervisory Correctional Officers, and Shift Rosters	As requested by COR
86	Overnight lodging requests	Advance of commencement of overnight trip
87	Non-returned ID Badges/Credentials	Immediately to COR
88	Intelligence Information	Immediately to COR
89	Serious Incidents	Immediately to COR

Section E

90	Contractor Employee Manual	Within 30 calendar days of award of contract and after that anytime as requested by the COR.
91	Any requested Detainee medical documentation	Immediately to COR
92	Medical and Personnel Records of Contractor Employees	As requested by COR
93	Contractor Business Permits and Licenses	Within 30 calendar days of award of contract and after that anytime as directed by COR.
94	Contractor Employee Registrations, Commissions, Permits, and Licenses	Prior to EOD and then after, as requested by COR
95	Correctional Officer Post Assignment Record	As requested by COR
96	Count Records	As requested by COR
97	GSA Form 139 or ICE equivalent	As requested by COR
98	Authorization to exceed a change in duty	To COR for approval prior to commencement of change of duty
99	Lost and Found	As requested by COR
100	Security incidents – computers	To COR within four (4) hours of incident
101	Daily Detainee Manifest	As requested by COR
102	Contract Discrepancy Report, Corrective Action Plan, or outcome measures required by any inspection or accreditation review, QASP or PBNDS requirements	As outlined within the requiring document

Section E

103	Spill Report	Immediately to COR
104	Transition-Out	1 week after notification of Transition to New Vendor
105	Small Business Subcontracting Plan	Submitted with Proposal
106	Operational Data/Metrics Summary	Due within three (3) days of request

** The word “immediately” or “immediate,” as used above in the Deliverables Chart is defined as “as soon as reasonably possible”. The Contractor should use prudent and reasonable judgement to determine the timeframe necessary to notify the Government as defined above based on the situation, but it should not exceed a reasonable timeframe to notify the Government. For example, a reasonable timeframe for a physical force incident is as soon as the incident that required a physical force response has been contained. A reasonable timeframe to notify the Government of an attempted escape is after the detainee is safely within the confines of the building. A reasonable timeframe to report an actual escape in which the Contractor does not know the location of the detainee is as soon as the Contractor realizes there has been an escape. In the case of a conflict between the Program Office and the Contractor on a reasonable timeframe, the Contracting Officer will determine the appropriate reasonable timeframe.*

E.4 ACCEPTANCE CRITERIA

The Government will provide written notification of acceptance or rejection of all final deliverables within thirty (30) calendar days. Absent written notification, final deliverables may be construed as accepted. All notifications of rejection will be accompanied with an explanation of the specific deficiencies causing the rejection.

[THE BALANCE OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

[END OF SECTION E]

Section F

SECTION F: DELIVERIES OR PERFORMANCE

F.1 CLAUSES INCORPORATED BY REFERENCE (FAR 52.252-2) (FEB 1998)

This contract incorporates the following clauses by reference with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text can be accessed electronically at this internet address: <http://acquisition.gov/far/index.html>.

Clause Number	Clause Title	Date
52.242-15	Stop Work Order	Aug 1989
52.242-17	Government Delay of Work	Apr 1984

F.2 PERIOD OF PERFORMANCE

The period of performance for this requirement is as follows:

Period of Performance	Dates
Base Period	08/06/2020 - 08/05/2021
<i>In Accordance with FAR 52.217-9</i>	
Option 1	08/06/2021 - 08/05/2022
Option 2	08/06/2022 - 08/05/2023
Option 3	08/06/2023 - 08/05/2024
Option 4	08/06/2024 - 08/05/2025
Option 5	08/06/2025 - 08/05/2026
Option 6	08/06/2026 - 08/05/2027
Option 7	08/06/2027 - 08/05/2028
Option 8	08/06/2028 - 08/05/2029
Option 9	08/06/2029 - 08/05/2030

F.3 PLACE OF PERFORMANCE:

*South Texas ICE Processing Center
566 Veterans Dr.
Pearsall, TX 78061*

No single facility described below should provide housing of less than 250 adults. The facilities' requirements are as follows:

- One facility or several facilities shall house approximately 2,000 adult male and female detainees within the San Antonio AOR. The facility shall be located within 75 miles from the San Antonio Field Office located at 1700 NE Loop 410, San Antonio Texas 78217, to

Section F

maximize transportation and manpower efficiencies, and no more than 30 driving miles from a major hospital and emergency services. The facility(ies) shall have access to public and commercial transportation routes and services and must be located 90 driving miles or less from San Antonio International Airport (SAT). The facility(ies) is (are) expected to house Level 1, 2, and 3 risk detainees. Please see the PWS Addendum B for additional specific requirements.

The facility shall be managed and operable 24 hours a day, 7 days a week for 365 days a year and 366 days a year for any leap years. The services shall be conducted in accordance with industry standards and ICE's Performance Based National Detention Standards (PBNDS) 2011, as revised in 2016, as well as applicable federal, state, and local laws, regulations, codes, guidelines, policies and standards. The facilities must meet the requirements of the DHS Final Rule, 6 CFR Part 115, Standards to Prevent, Detect, and Respond to Sexual Abuse and Assault in Confinement Facilities, also known as the DHS Prison Rape Elimination Act (PREA) Standards applicable to immigration detention facilities.

F.4 CONTRACTOR EVALUATING PROCEDURES:

The Government will issue Contractor performance ratings for each awarded requirement from this solicitation via the Contractor Performance Assessment Reporting System (CPARS) in accordance with FAR 42.1502. The CPARS website is located: <http://www.cpars.gov>.

[THE BALANCE OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

[END OF SECTION F]

SECTION G: CONTRACT ADMINISTRATION DATA

G.1 CONTRACT ADMINISTRATION

Notwithstanding the Contractor's responsibility for total management responsibility during the performance of this contract, the administration of the contract will require maximum coordination between the ICE and the Contractor.

The Government points of contact for this resulting contract are identified above.

G.2 CONTRACTING OFFICER'S REPRESENTATIVE

The following individual is designated and authorized by the CO to perform contract administration functions related to the technical performance of this contract.

The Government points of contact for this resulting contract are identified above.

(a) The Contracting Officer (CO) may designate Government personnel to act as the Contracting Officer's Representative (COR) to perform functions under the contract such as review or inspection and acceptance of supplies, services, including construction, and other functions of a technical nature. The CO will provide a written notice of such designation to the Contractor within five working days after contract award or for construction, not less than five working days prior to giving the contractor the notice to proceed. The designation letter will set forth the authorities and limitations of the COR under the contract.

(b) The CO cannot authorize the COR or any other representative to sign documents, such as contracts, contract modifications, etc., that require the signature of the CO.

G.3 INVOICE REQUIREMENTS

Invoices shall be submitted as follows:

Service Providers/Contractors shall use these procedures when submitting an invoice.

1. Invoice Submission: Invoices shall be submitted monthly in a ".pdf" format in accordance with the contract terms and conditions via email, United States Postal Service (USPS) or facsimile as follows:

a) Email:

- (b) (7)(E) [REDACTED]@ice.dhs.gov
- Contracting Officer Representative (COR) or Government Point of Contact (GPOC)

Section G

- Contract Specialist/Contracting Officer

Each email shall contain only (1) invoice and the invoice number shall be indicated on the subject line of the email.

b) USPS:

DHS, ICE
Financial Operations - Burlington
P.O. Box 1620
Williston, VT 05495-1620

ATTN: ICE-ERO-FOD-FAO

The Contractors Data Universal Numbering System (DUNS) Number must be registered and active in the System for Award Management (SAM) at <https://www.sam.gov> prior to award and shall be notated on every invoice submitted to ensure prompt payment provisions are met. The ICE program office identified in the task order/contract shall also be notated on every invoice.

c) Facsimile:

Alternative Invoices shall be submitted to: (802)-288-7658

Submissions by facsimile shall include a cover sheet, point of contact and the number of total pages.

Note: The Service Provider's or Contractor's Dunn and Bradstreet (D&B) DUNS Number must be registered in the System for Award Management (SAM) at <https://www.sam.gov> prior to award and shall be notated on every invoice submitted to ensure prompt payment provisions are met. The ICE program office identified in the task order/contract shall also be notated on every invoice.

2. Content of Invoices: Each invoice shall contain the following information in accordance with 52.212-4 (g), as applicable:

(i). Name and address of the Service Provider/Contractor. Note: the name, address and DUNS number on the invoice MUST match the information in both the Contract/Agreement and the information in the SAM. If payment is remitted to another entity, the name, address and DUNS information of that entity must also be provided which will require Government verification before payment can be processed;

(ii). Dunn and Bradstreet (D&B) DUNS Number;

(iii). Invoice date and invoice number;

Section G

- (iv). Agreement/Contract number, contract line item number and, if applicable, the order number;
- (v). Description, quantity, unit of measure, unit price, extended price and period of performance of the items or services delivered;
- (vi). If applicable, shipping number and date of shipment, including the bill of lading number and weight of shipment if shipped on Government bill of lading;
- (vii). Terms of any discount for prompt payment offered;
- (viii). Remit to Address;
- (ix). Name, title, and phone number of person to resolve invoicing issues;
- (x). ICE program office designated on order/contract/agreement and
- (xi). Mark invoice as “Interim” (Ongoing performance and additional billing expected) and “Final” (performance complete and no additional billing)
- (xii). Electronic Funds Transfer (EFT) banking information in accordance with 52.232-33 Payment by Electronic Funds Transfer – System for Award Management or 52-232-34, Payment by Electronic Funds Transfer – Other than System for Award Management.

3. Invoice Supporting Documentation. To ensure payment, the vendor must submit supporting documentation which provides substantiation for the invoiced costs to the Contracting Officer Representative (COR) or Point of Contact (POC) identified in the contract. Invoice charges must align with the contract CLINs. Supporting documentation is required when guaranteed minimums are exceeded and when allowable costs are incurred. Details are as follows:

- (i). Guaranteed Minimums. If a guaranteed minimum is not exceeded on a CLIN(s) for the invoice period, no supporting documentation is required. When a guaranteed minimum is exceeded on a CLIN (s) for the invoice period, the Contractor is required to submit invoice supporting documentation for all detention services provided during the invoice period which provides the information described below:
 - a. Detention Bed Space Services
 - Bed day rate;
 - Detainees check-in and check-out dates;
 - Number of bed days multiplied by the bed day rate;
 - Name of each detainee;
 - Detainees identification information
- (ii). Allowable Incurred Cost. Fixed Unit Price Items (items for allowable incurred costs, such as transportation services, stationary guard or escort services, transportation mileage or other

Section G

Minor Charges such as sack lunches and detainee wages): shall be fully supported with documentation substantiating the costs and/or reflecting the established price in the contract and shall be submitted in .pdf format:

a. Detention Bed Space Services. For detention bed space CLINs without a GM, the supporting documentation must include:

- Bed day rate;
- Detainees check-in and check-out dates;
- Number of bed days multiplied by the bed day rate;
- Name of each detainee;
- Detainees identification information

b. Transportation Services: For transportation CLINs without a GM, the supporting documentation must include:

- Mileage rate being applied for that invoice;
- Number of miles;
- Transportation routes provided;
- Locations serviced;
- Names of detainees transported;
- Itemized listing of all other charges; and,
- for reimbursable expenses (e.g. travel expenses, special meals, etc.) copies of all receipts.

c. Stationary Guard Services: The itemized monthly invoice shall state:

- The location where the guard services were provided,
- The employee guard names and number of hours being billed,
- The employee guard names and duration of the billing (times and dates), and
- for individual or detainee group escort services only, the name of the detainee(s) that was/were escorted.

d. Other Direct Charges (e.g. VTC support, transportation meals/sack lunches, volunteer detainee wages, etc.):

1) The invoice shall include appropriate supporting documentation for any direct charge billed for reimbursement. For charges for detainee support items (e.g. meals, wages, etc.), the supporting documentation should include the name of the detainee(s) supported and the date(s) and amount(s) of support.

(iii) Firm Fixed-Price CLINs. Supporting documentation is not required for charges for FFP CLINs.

4. Safeguarding Information: As a contractor or vendor conducting business with Immigration and Customs Enforcement (ICE), you are required to comply with DHS Policy regarding the safeguarding of Sensitive Personally Identifiable Information (PII). Sensitive PII is information that identifies an individual, including an alien, and could result in harm, embarrassment, inconvenience or unfairness. Examples of Sensitive PII include information

Section G

such as: Social Security Numbers, Alien Registration Numbers (A-Numbers), or combinations of information such as the individuals name or other unique identifier and full date of birth, citizenship, or immigration status.

As part of your obligation to safeguard information, the follow precautions are required:

- (i) Email supporting documents containing Sensitive PII in an encrypted attachment with password sent separately to the Contracting Officer Representative assigned to the contract.
- (ii) Never leave paper documents containing Sensitive PII unattended and unsecure. When not in use, these documents will be locked in drawers, cabinets, desks, etc. so the information is not accessible to those without a need to know.
- (iii) Use shredders when discarding paper documents containing Sensitive PII.
- (iv) Refer to the DHS Handbook for Safeguarding Sensitive Personally Identifiable Information (March 2012) found at <http://www.dhs.gov/xlibrary/assets/privacy/dhs-privacy-safeguardingsensitivepiihandbook-march2012.pdf> for more information on and/or examples of Sensitive PII.

5. Invoice Inquiries. If you have questions regarding payment, please contact ICE Financial Operations at 1-877-491-6521 or by e-mail at [\(b\) \(7\)\(E\) Service@ice.dhs.gov](mailto:(b) (7)(E) Service@ice.dhs.gov).

Invoices without the above information may be returned for resubmission.

The preferred method of submittal is email.

[THE BALANCE OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

[END OF SECTION G]

SECTION H: SPECIAL CONTRACT REQUIREMENTS

H.1. CONTRACTOR'S INSURANCE

The Contractor shall maintain insurance in an amount not less than (b) (3) (A), (b) (4) to protect the Contractor from claims under workman's compensation acts and from any other claims for damages for personal injury, including death which may arise from operations under this contract whether such operations by the Contractor itself or by any subcontractor or anyone directly or indirectly employed by either business entity. The Contractor shall maintain General Liability insurance; bodily injury liability coverage written on a comprehensive form of policy of at least (b) (3) (A), (b) (4) per occurrence is required.

Additionally, an automobile liability insurance policy providing for bodily injury and property damage liability covering automobiles operated in the United States shall provide coverage of at least (b) (3) (A), (b) (4) per person and (b) (3) (A), (b) (4) per occurrence for bodily injury and (b) (3) (A), (b) (4) per occurrence for property coverage. Certificates of such insurance shall be subject to the approval of the CO for adequacy of protection. All insurance certificates required under this contract shall provide (b) (3) (A), (b) (4) days' notice to the Government of any contemplated cancellation.

The Contractor shall provide that all staff having access to detainee monies and valuables are bonded in an amount sufficient to ensure reimbursement to the detainee by the Contractor in case of loss.

H.2. SECURITY REQUIREMENTS - REQUIRED SECURITY LANGUAGE FOR SENSITIVE /BUT UNCLASSIFIED (SBU) CONTRACT DETENTION FACILITY

General: Performance under this Contract Detention Facility requires access to sensitive DHS information and will involve direct contact with ICE Detainees. The Contractor shall adhere to the following.

Contractor Employee Fitness Screening: Screening criteria under DHS Instruction 121-01-007-001 (Personnel Security, Suitability and Fitness Program), or successor thereto, that may exclude contractor employees from consideration to perform under this agreement includes:

- Misconduct or negligence in employment;
- Criminal or dishonest conduct;
- Material, intentional false statement or deception of fraud in examination or appointment;
- Refusal to furnish testimony as required by 5 CFR § 5.4 (i.e., a refusal to provide testimony to the Merit Systems Protection Board or the Office of Special Counsel);
- Illegal use of narcotics, drugs, or other controlled substances without evidence of substantial rehabilitation.
- Alcohol abuse, without evidence of substantial rehabilitation, of a nature and duration that suggests that the applicant or appointee would be prevented from performing the

Section H

duties of the position in question, or would constitute a direct threat to the property or safety of the applicant or appointee or others;

- Illegal use of narcotics, drugs, or other controlled substances, without evidence of substantial rehabilitation;
- Knowing and willful engagement in acts or activities designed to overthrow the U.S. Government by force;
- Any statutory or regulatory bar which prevents the lawful employment of the person involved in the position in question (for Excepted Service employees); and
- Any other nondiscriminatory reason that an individual's employment (or work on a contract) would not protect the integrity of promote the efficiency of the service.

Contractor Employee Fitness Screening: Screening criteria under 6 CFR § 115.117 (Sexual Abuse and Assault Prevention Standards) implemented pursuant to Public Law 108-79 (Prison Rape Elimination Act (PREA) of 2003) or successor thereto, that WILL exclude contractor employees from consideration to perform under this agreement includes:

- Engaged in Sexual Abuse in a Prison, Jail, Holding Facility, Community Confinement Facility, Juvenile Facility, or other Institution as defined under 42 USC 1997;
- Convicted of engaging or attempting to engage in sexual activity facilitated by force, overt or implied threats of force, or coercion, or if the victim did not consent or was unable to consent or refuse;
- Civilly or administratively adjudicated to have in engaged in such activity.

Subject to existing law, regulations and/or other provisions of this Agreement, illegal or undocumented aliens shall not be employed by the Service Provider.

1.2.1 GENERAL

The United States Immigration and Customs Enforcement (ICE) has determined that performance of the tasks as described in contract agreement (#) 70CDCR20D00000012 requires that the Contractor, subcontractor(s), vendor(s), etc. (herein known as Contractor) have access to sensitive DHS information and ICE Detainees, and that the Contractor will adhere to the following:

1.2.2 PRELIMINARY FITNESS DETERMINATION

ICE will exercise full control over granting, denying, withholding or terminating unescorted government facility and/or sensitive Government information access for contractor employees, based upon the results of a Fitness screening process. ICE may, as it deems appropriate, authorize and make a favorable expedited preliminary Fitness determination based on preliminary security checks. The preliminary Fitness determination will allow the contractor employee to commence work temporarily prior to the completion of a Full Field Background Investigation. The granting of a favorable preliminary Fitness shall not be considered as assurance that a favorable final Fitness determination will follow as a result thereof. The granting of preliminary Fitness or final Fitness shall in no way prevent, preclude, or bar the withdrawal or termination of any such access by ICE, at any time during the term of the contract. No employee

Section H

of the Contractor shall be allowed to enter on duty and/or access sensitive information or systems without a favorable preliminary Fitness determination or final Fitness determination by the Office of Professional Responsibility, Personnel Security Unit (OPR-PSU). No employee of the Contractor shall be allowed unescorted access to a Government facility without a favorable preliminary Fitness determination or final Fitness determination by OPR-PSU. Contractor employees are processed under DHS Instruction 121-01-007-001 (Personnel Security, Suitability and Fitness Program), or successor thereto; those having direct contact with Detainees will also have 6 CFR § 115.117 considerations made as part of the Fitness screening process.

1.2.3 BACKGROUND INVESTIGATIONS

Contractor employees (to include applicants, temporaries, part-time and replacement employees) under the contract, needing access to sensitive information and/or ICE Detainees, shall undergo a position sensitivity analysis based on the duties each individual will perform on the contract. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. Background investigations will be processed through the Personnel Security Unit. Contractor employees nominated by a Contracting Officer Representative for consideration to support this contract shall submit the following security vetting documentation to OPR-PSU, through the Contracting Officer Representative (COR), within 10 days of notification by OPR-PSU of nomination by the COR and initiation of an Electronic Questionnaire for Investigation Processing (e-QIP) in the Office of Personnel Management (OPM) automated on-line system.

1. Standard Form 85P (Standard Form 85PS (With supplement to 85P required for armed positions)), "Questionnaire for Public Trust Positions" Form completed on-line and archived by the contractor employee in their OPM e-QIP account.
2. Signature Release Forms (Three total) generated by OPM e-QIP upon completion of Questionnaire (e-signature recommended/acceptable – instructions provided to applicant by OPR-PSU). Completed on-line and archived by the contractor employee in their OPM e-QIP account.
3. Two (2) SF 87 (Rev. December 2017) Fingerprint Cards. **(Two Original Cards sent via COR to OPR-PSU)**
4. Foreign National Relatives or Associates Statement. (This document sent as an attachment in an e-mail to contractor employee from OPR-PSU – must be signed and archived into contractor employee's OPM e-QIP account prior to electronic "Release" of data via on-line account)
5. DHS 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act" (This document sent as an attachment in an e-mail to contractor employee from OPR-PSU – must be signed and archived into contractor employee's OPM e-QIP account prior to electronic "Release" of data via on-line account)

Section H

6. Optional Form 306 Declaration for Federal Employment (This document sent as an attachment in an e-mail to contractor employee from OPR-PSU – must be signed and archived into contractor employee’s OPM e-QIP account prior to electronic “Release” of data via on-line account)
7. Questionnaire regarding conduct defined under 6 CFR § 115.117 (Sexual Abuse and Assault Prevention Standards) (This document sent as an attachment in an e-mail to contractor employee from OPR-PSU – must be signed and archived into contractor employee’s OPM e-QIP account prior to electronic “Release” of data via on-line account)
8. One additional document may be applicable if contractor employee was born abroad. If applicable, additional form and instructions will be provided to contractor employee. (If applicable, the document will be sent as an attachment in an e-mail to contractor employee from OPR-PSU – must be signed and archived into contractor employee’s OPM e-QIP account prior to electronic “Release” of data via on-line account)

Contractor employees who have an adequate, current investigation by another Federal Agency may not be required to submit complete security packages; the investigation may be accepted under reciprocity. The questionnaire related to 6 CFR § 115.117 listed above in item 7 will be required for positions designated under PREA.

An adequate and current investigation is one where the investigation is not more than five years old, meets the contract risk level requirement, and applicant has not had a break in service of more than two years. (Executive Order 13488 amended under Executive Order 13764/DHS Instruction 121-01-007-01).

Required information for submission of security packet will be provided by OPR-PSU at the time of award of the contract. Only complete packages will be accepted by the OPR-PSU as notified by the COR.

To ensure adequate background investigative coverage, contractor employees must currently reside in the United States or its Territories. Additionally, contractor employees are required to have resided within the United States or its Territories for three or more years out of the last five (ICE retains the right to deem a contractor employee ineligible due to insufficient background coverage). This timeline is assessed based on the signature date of the standard form questionnaire submitted for the applied position. Contractor employees falling under the following situations may be exempt from the residency requirement: 1) work or worked for the U.S. Government in foreign countries in federal civilian or military capacities; 2) were or are dependents accompanying a federal civilian or a military employee serving in foreign countries so long as they were or are authorized by the U.S. Government to accompany their federal civilian or military sponsor in the foreign location; 3) worked as a contractor employee, volunteer, consultant or intern on behalf of the federal government overseas, where stateside coverage can be obtained to complete the background investigation; 4) studied abroad at a U.S. affiliated college or university; or 5) have a current and adequate background investigation (commensurate with the position risk/sensitivity levels) completed for a federal or contractor employee position, barring any break in federal employment or federal sponsorship.

Section H

Only U.S. Citizens and Legal Permanent Residents are eligible for employment on contracts requiring access to DHS sensitive information unless an exception is granted as outlined under DHS Instruction 121-01-007-001. Per DHS Sensitive Systems Policy Directive 4300A, only U.S. citizens are eligible for positions requiring access to DHS Information Technology (IT) systems or positions that are involved in the development, operation, management, or maintenance of DHS IT systems, unless an exception is granted as outlined under DHS Instruction 121-01-007-001.

1.2.4 TRANSFERS FROM OTHER DHS CONTRACTS:

Contractor employees may be eligible for transfer from other DHS Component contracts provided they have an adequate and current investigation meeting the new assignment requirement. If the contractor employee does not meet the new assignment requirement a DHS 11000-25 with ICE supplemental page will be submitted to OPR-PSU to initiate a new investigation.

Transfers will be accomplished by submitting a DHS 11000-25 with ICE supplemental page indicating "Contract Change." The questionnaire related to 6 CFR § 115.117 listed above in item 7 will be required for positions designated under PREA.

1.2.5 CONTINUED ELIGIBILITY

ICE reserves the right and prerogative to deny and/or restrict facility and information access of any contractor employee whose actions conflict with Fitness standards contained in DHS Instruction 121-01-007-01, Chapter 3, paragraph 6.B or who violate standards of conduct under 6 CFR § 115.117. The Contracting Officer or their representative can determine if a risk of compromising sensitive Government information exists or if the efficiency of service is at risk and may direct immediate removal of a contractor employee from contract support. The OPR-PSU will conduct periodic reinvestigations every 5 years, or when derogatory information is received, to evaluate continued Fitness of contractor employees.

1.2.6 REQUIRED REPORTS

The Contractor will notify OPR-PSU, via the COR, of all terminations/resignations of contractor employees under the contract within five days of occurrence. The Contractor will return any expired ICE issued identification cards and building passes of terminated/ resigned employees to the COR. If an identification card or building pass is not available to be returned, a report must be submitted to the COR referencing the pass or card number, name of individual to whom issued, the last known location and disposition of the pass or card. The COR will return the identification cards and building passes to the responsible ID Unit.

The Contractor will report any adverse information coming to their attention concerning contractor employees under the contract to the OPR-PSU, via the COR, as soon as possible. Reports based on rumor or innuendo should not be made. The subsequent termination of employment of an employee does not obviate the requirement to submit this report. The report

Section H

shall include the contractor employees' name and social security number, along with the adverse information being reported.

The Contractor will provide, through the COR a Quarterly Report containing the names of contractor employees who are active, pending hire, have departed within the quarter or have had a legal name change (Submitted with documentation). The list shall include the Name, Position and SSN (Last Four) and should be derived from system(s) used for contractor payroll/voucher processing to ensure accuracy.

CORs will submit reports to (b) (7)(E) @ice.dhs.gov

Contractors, who are involved with management and/or use of information/data deemed "sensitive" to include "law enforcement sensitive" are required to complete the DHS Form 11000-6-Sensitive but Unclassified Information NDA for contractor access to sensitive information. The NDA will be administered by the COR to the all contract personnel within 10 calendar days of the entry on duty date. The completed form shall remain on file with the COR for purpose of administration and inspection.

Sensitive information as defined under the Computer Security Act of 1987, Public Law 100-235 is information not otherwise categorized by statute or regulation that if disclosed could have an adverse impact on the welfare or privacy of individuals or on the welfare or conduct of Federal programs or other programs or operations essential to the national interest. Examples of sensitive information include personal data such as Social Security numbers; trade secrets; system vulnerability information; pre-solicitation procurement documents, such as statements of work; and information pertaining to law enforcement investigative methods; similarly, detailed reports related to computer security deficiencies in internal controls are also sensitive information because of the potential damage that could be caused by the misuse of this information. All sensitive information must be protected from loss, misuse, modification, and unauthorized access in accordance with DHS Management Directive 11042.1, *DHS Policy for Sensitive Information* and ICE Policy 4003, *Safeguarding Law Enforcement Sensitive Information.*"

Any unauthorized disclosure of information should be reported to (b) (7)(E) @ICE.dhs.gov.

1.2.7 SECURITY MANAGEMENT

The Contractor shall appoint a senior official to act as the Corporate Security Officer. The individual will interface with the OPR-PSU through the COR on all security matters, to include physical, personnel, and protection of all Government information and data accessed by the Contractor.

The COR and the OPR-PSU shall have the right to inspect the procedures, methods, and facilities utilized by the Contractor in complying with the security requirements under this contract. Should the COR determine that the Contractor is not complying with the security requirements of this contract, the Contractor will be informed in writing by the Contracting Officer of the proper action to be taken in order to effect compliance with such requirements.

The computer security requirements as described in paragraphs 1.2.8 and 1.2.9 of this section

Section H

apply to both Department of Homeland Security (DHS) U.S. Immigration and Customs Enforcement (ICE) operations and to the former Immigration and Naturalization Service operations (FINS). These entities are hereafter referred to as the Department.

1.2.8 INFORMATION TECHNOLOGY SECURITY CLEARANCE

When sensitive government information is processed on Department telecommunications and automated information systems, the Contractor agrees to provide for the administrative control of sensitive data being processed and to adhere to the procedures governing such data as outlined in DHS MD 4300.1, *Information Technology Systems Security*, or its replacement. Contractor employees must have favorably adjudicated background investigations commensurate with the defined sensitivity level.

Contractor employees who fail to comply with Department security policy are subject to having their access to Department IT systems and facilities terminated, whether or not the failure results in criminal prosecution. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions under a variety of laws (e.g., Privacy Act).

1.2.9 INFORMATION TECHNOLOGY SECURITY TRAINING AND OVERSIGHT

In accordance with Chief Information Office requirements and provisions, all contractor employees accessing Department IT systems or processing DHS sensitive data via an IT system will require an ICE issued/provisioned Personal Identity Verification (PIV) card. Additionally, Information Assurance Awareness Training (IAAT) will be required upon initial access and annually thereafter. IAAT training will be provided by the appropriate component agency of DHS.

Contractor employees, who are involved with management, use, or operation of any IT systems that handle sensitive information within or under the supervision of the Department, shall receive periodic training at least annually in security awareness and accepted security practices, systems rules of behavior, to include Unauthorized Disclosure Training, available on PALMS or by contacting (b) (7)(E) @ICE.dhs.gov. Department contractor employees, with significant security responsibilities, shall receive specialized training specific to their security responsibilities annually. The level of training shall be commensurate with the individual's duties and responsibilities and is intended to promote a consistent understanding of the principles and concepts of telecommunications and IT systems security.

All personnel who access Department information systems will be continually evaluated while performing these duties. System Administrators should be aware of any unusual or inappropriate behavior by personnel accessing systems. Any unauthorized access, sharing of passwords, or other questionable security procedures should be reported to the local Security Office or Information System Security Officer (ISSO).

H.3. ICE INFORMATION GOVERNANCE AND PRIVACY REQUIREMENTS CLAUSE (JUL 2017)

Section H

No section of this clause may be read as self-deleting unless the terms of the contract meet the requirements for self-deletion as specified in this clause.

A. Limiting Access to Privacy Act and Other Sensitive Information

(1) Privacy Act Information

In accordance with FAR 52.224-1 Privacy Act Notification (APR 1984), and FAR 52.224-2 Privacy Act (APR 1984), if this contract requires contractor personnel to have access to information protected by the Privacy Act of 1974 the contractor is advised that the relevant DHS system of records notices (SORNs) applicable to this Privacy Act information may be found at www.dhs.gov/privacy. Applicable SORNS of other agencies may be accessed through the agencies' websites or by searching FDsys, the Federal Digital System, available at <http://www.gpo.gov/fdsys/>. SORNs may be updated at any time.

(3) Prior Approval Required to Hire Subcontractors

The Contractor is required to obtain the Contracting Officer's approval prior to engaging in any contractual relationship (Subcontractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under or relating to this contract. The Contractor (and any Subcontractor) is required to abide by Government and Agency guidance for protecting sensitive and proprietary information.

(4) Separation Checklist for Contractor Employees

Contractor shall complete a separation checklist before any employee or Subcontractor employee terminates working on the contract. The separation checklist must verify: (1) return of any Government-furnished equipment; (2) return or proper disposal of sensitive personally identifiable information (PII), in paper or electronic form, in the custody of the employee or Subcontractor employee including the sanitization of data on any computer systems or media as appropriate; and (3) termination of any technological access to the Contractor's facilities or systems that would permit the terminated employee's access to sensitive PII.

In the event of adverse job actions resulting in the dismissal of an employee or Subcontractor employee, the Contractor shall notify the Contracting Officer's Representative (COR) within 24 hours. For normal separations, the Contractor shall submit the checklist on the last day of employment or work on the contract.

As requested, contractors shall assist the ICE Point of Contact (ICE/POC), Contracting Officer, or COR with completing ICE Form 50-005/Contractor Employee Separation Clearance Checklist by returning all Government-furnished property including but not limited to computer equipment, media, credentials and passports, smart cards, mobile devices, PIV cards, calling cards, and keys and terminating access to all user accounts and systems.

B. Privacy Training, Safeguarding, and Remediation

If the Safeguarding of Sensitive Information (MAR 2015) and Information Technology Security and Privacy Training (MAR 2015) clauses are included in this contract, section B of

Section H

this clause is deemed self-deleting.

(1) Required Security and Privacy Training for Contractors

Contractor shall provide training for all employees, including Subcontractors and independent contractors who have access to sensitive personally identifiable information (PII) as well as the creation, use, dissemination and/or destruction of sensitive PII at the outset of the employee's work on the contract and every year thereafter. Training must include procedures on how to properly handle sensitive PII, including security requirements for the transporting or transmission of sensitive PII, and reporting requirements for a suspected breach or loss of sensitive PII. All Contractor employees are required to take the *Privacy at DHS: Protecting Personal Information* training course. This course, along with more information about DHS security and training requirements for Contractors, is available at www.dhs.gov/dhs-security-and-training-requirements-contractors. The Federal Information Security Management Act (FISMA) requires all individuals accessing ICE information to take the annual Information Assurance Awareness Training course. These courses are available through the ICE intranet site or the Agency may also make the training available through hypertext links or CD. The Contractor shall maintain copies of employees' certificates of completion as a record of compliance and must submit an annual e-mail notification to the ICE Contracting Officer's Representative that the required training has been completed for all the Contractor's employees.

(2) Safeguarding Sensitive PII Requirement

Contractor employees shall comply with the Handbook for Safeguarding sensitive PII at DHS at all times when handling sensitive PII, including the encryption of sensitive PII as required in the Handbook. This requirement will be flowed down to all subcontracts and lower tiered subcontracts as well.

(3) Non-Disclosure Agreement Requirement

All Contractor personnel that may have access to PII or other sensitive information shall be required to sign a Non-Disclosure Agreement (DHS Form 11000-6) prior to commencing work. The Contractor shall maintain signed copies of the NDA for all employees as a record of compliance. The Contractor shall provide copies of the signed NDA to the Contracting Officer's Representative (COR) no later than two (2) days after execution of the form.

(4) Prohibition on Use of PII in Vendor Billing and Administrative Records

The Contractor's invoicing, billing, and other financial/administrative records/databases may not store or include any sensitive Government information, such as PII that is created, obtained, or provided during the performance of the contract. It is acceptable to list the names, titles and contact information for the Contracting Officer, Contracting Officer's Representative, or other ICE personnel associated with the administration of the contract in the invoices as needed.

(5) Reporting Suspected Loss of Sensitive PII

Contractors must report the suspected loss or compromise of sensitive PII to ICE in a timely manner and cooperate with ICE's inquiry into the incident and efforts to remediate any harm to potential victims.

1. The Contractor must develop and include in its security plan (which is submitted to ICE) an

Section H

internal system by which its employees and Subcontractors are trained to identify and report the potential loss or compromise of sensitive PII.

2. The Contractor must report the suspected loss or compromise of sensitive PII by its employees or Subcontractors to the ICE Security Operations Center (480-496-6627), the Contracting Officer's Representative (COR), and the Contracting Officer within one (1) hour of the initial discovery.

3. The Contractor must provide a written report to ICE within 24 hours of the suspected loss or compromise of sensitive PII by its employees or Subcontractors. The report must contain the following information:

- a. Narrative or detailed description of the events surrounding the suspected loss or compromise of information.
- b. Date, time, and location of the incident.
- c. Type of information lost or compromised.
- d. Contractor's assessment of the likelihood that the information was compromised or lost and the reasons behind the assessment.
- e. Names of person(s) involved, including victim, Contractor employee/Subcontractor and any witnesses.
- f. Cause of the incident and whether the company's security plan was followed and, if not, which specific provisions were not followed.
- g. Actions that have been or will be taken to minimize damage and/or mitigate further compromise.
- h. Recommendations to prevent similar situations in the future, including whether the security plan needs to be modified in any way and whether additional training may be required.

4. The Contractor shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents.

5. At the Government's discretion, Contractor employees or Subcontractor employees may be identified as no longer eligible to access sensitive PII or to work on that contract based on their actions related to the loss or compromise of sensitive PII.

(6) Victim Remediation

The Contractor is responsible for notifying victims and providing victim remediation services in the event of a loss or compromise of sensitive PII held by the Contractor, its agents, or its Subcontractors, under this contract. Victim remediation services shall include at least 18 months of credit monitoring and, for serious or large incidents as determined by the Government, call center help desk services for the individuals whose sensitive PII was lost or compromised. The Contractor and ICE will collaborate and agree on the method and content of any notification that may be required to be sent to individuals whose sensitive PII was lost or compromised.

Section H

C. Government Records Training, Ownership, and Management

(1) Records Management Training and Compliance

(a) The Contractor shall provide DHS basic records management training for all employees and Subcontractors that have access to sensitive PII as well as to those involved in the creation, use, dissemination and/or destruction of sensitive PII. This training will be provided at the outset of the Subcontractor's/employee's work on the contract and every year thereafter. This training can be obtained via links on the ICE intranet site or it may be made available through other means (e.g., CD or online). The Contractor shall maintain copies of certificates as a record of compliance and must submit an e-mail notification annually to the Contracting Officer's Representative verifying that all employees working under this contract have completed the required records management training.

(b) The Contractor agrees to comply with Federal and Agency records management policies, including those policies associated with the safeguarding of records covered by the Privacy Act of 1974. These policies include the preservation of all records created or received regardless of format, mode of transmission, or state of completion.

(2) Records Creation, Ownership, and Disposition

(a) The Contractor shall not create or maintain any records not specifically tied to or authorized by the contract using Government IT equipment and/or Government records or that contain Government Agency data. The Contractor shall certify in writing the destruction or return of all Government data at the conclusion of the contract or at a time otherwise specified in the contract.

(b) Except as stated in the Performance Work Statement and, where applicable, the Contractor's Commercial License Agreement, the Government Agency owns the rights to all electronic information (electronic data, electronic information systems or electronic databases) and all supporting documentation and associated metadata created as part of this contract. All deliverables (including all data and records) under the contract are the property of the U.S. Government and are considered federal records, for which the Agency shall have unlimited rights to use, dispose of, or disclose such data contained therein. The Contractor must deliver sufficient technical documentation with all data deliverables to permit the agency to use the data.

(c) The Contractor shall not retain, use, sell, disseminate, or dispose of any government data/records or deliverables without the express written permission of the Contracting Officer or Contracting Officer's Representative. The Agency and its contractors are responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. § 2701. Records may not be removed from the legal custody of the Agency or destroyed without regard to the provisions of the Agency records schedules.

D. Data Privacy and Oversight

Section H

Section D applies to information technology (IT) contracts. If this is not an IT contract, section D may read as self-deleting.

(1) Restrictions on Testing or Training Using Real Data Containing PII

The use of real data containing sensitive PII from any source for testing or training purposes is generally prohibited. The Contractor shall use synthetic or de-identified real data for testing or training whenever feasible. ICE policy requires that any proposal to use of real data or de-identified data for IT system testing or training be approved by the ICE Privacy Officer and Chief Information Security Officer (CISO) in advance. In the event performance of the contract requires or necessitates the use of real data for system-testing or training purposes, the Contractor in coordination with the Contracting Officer or Contracting Officer's Representative and Government program manager shall obtain approval from the ICE Privacy Office and CISO and complete any required documentation.

If this IT contract contains the Safeguarding of Sensitive Information (MAR 2015) and Information Technology Security and Privacy Training (MAR 2015) clauses, section D(2) of this clause is deemed self-deleting.

(2) Requirements for Contractor IT Systems Hosting Government Data

The Contractor is required to obtain a Certification and Accreditation for any IT environment owned or controlled by the Contractor or any Subcontractor on which Government data shall reside for the purposes of IT system development, design, data migration, testing, training, maintenance, use, or disposal.

(3) Requirement to Support Privacy Compliance

(a) The Contractor shall support the completion of the Privacy Threshold Analysis (PTA) document when it is required. PTAs are triggered by the creation, modification, upgrade, or disposition of an IT system, and must be renewed at least every three years. Upon review of the PTA, the DHS Privacy Office determines whether a Privacy Impact Assessment (PIA) and/or Privacy Act System of Records Notice (SORN), or modifications thereto, are required. The Contractor shall provide adequate support to complete the PIA in a timely manner and shall ensure that project management plans and schedules include the PTA, PIA, and SORN (to the extent required) as milestones. Additional information on the privacy compliance process at DHS, including PTAs, PIAs, and SORNs, is located on the DHS Privacy Office website (www.dhs.gov/privacy) under "Compliance." DHS Privacy Policy Guidance Memorandum 2008-02 sets forth when a PIA will be required at DHS, and the Privacy Impact Assessment Guidance and Template outline the requirements and format for the PIA.

(b) If the contract involves an IT system build or substantial development or changes to an IT system that may require privacy documentation, the Contractor shall assign or procure a Privacy Lead, to be listed under "Key Personnel." The Privacy Lead shall be responsible for providing adequate support to DHS to ensure DHS can complete any required PTA, PIA, SORN, or other supporting documentation to support privacy compliance. The Privacy Lead shall work with personnel from the program office, the ICE Privacy Office, the Office of the Chief Information Officer, and the Records Management Branch to ensure that the privacy

Section H

documentation is kept on schedule, that the answers to questions in the PIA are thorough and complete, and that questions asked by the ICE Privacy Office and other offices are answered in a timely fashion. The Privacy Lead:

- Must have excellent writing skills, the ability to explain technology clearly for a non-technical audience, and the ability to synthesize information from a variety of sources.
- Must have excellent verbal communication and organizational skills.
- Must have experience writing PIAs. Ideally the candidate would have experience writing PIAs for DHS.
- Must be knowledgeable about the Privacy Act of 1974 and the E-Government Act of 2002.
- Must be able to work well with others.

(c) If a Privacy Lead is already in place with the program office and the contract involves IT system builds or substantial changes that may require privacy documentation, the requirement for a separate Private Lead specifically assigned under this contract may be waived provided the Contractor agrees to have the existing Privacy Lead coordinate with and support the ICE Privacy POC to ensure privacy concerns are proactively reviewed and so ICE can complete any required PTA, PIA, SORN, or other supporting documentation to support privacy compliance if required. The Contractor shall work with personnel from the program office, the ICE Office of Information Governance and Privacy, and the Office of the Chief Information Officer to ensure that the privacy documentation is kept on schedule, that the answers to questions in any privacy documents are thorough and complete, that all records management requirements are met, and that questions asked by the ICE Privacy Office and other offices are answered in a timely fashion.

H.4. INFORMATION TECHNOLOGY SECURITY AND PRIVACY TRAINING (MAR 2015)

(a) *Applicability.* This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as “Contractor”). The Contractor shall insert the substance of this clause in all subcontracts.

(b) *Security Training Requirements.*

(1) All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user’s responsibilities change. The Department of Homeland Security (DHS) requires that Contractor employees take an annual Information Technology Security Awareness Training course before accessing sensitive information under the contract. Unless otherwise specified, the training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall complete the training before accessing sensitive information under the contract. The training is accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor

Section H

employees as a record of compliance. Unless otherwise specified, initial training certificates for each Contractor and subcontractor employee shall be provided to the Contracting Officer's Representative (COR) not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(2) The DHS Rules of Behavior apply to every DHS employee, Contractor and subcontractor that will have access to DHS systems and sensitive information. The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable for actions taken while accessing DHS systems and using DHS Information Technology resources capable of inputting, storing, processing, outputting, and/or transmitting sensitive information. The DHS Rules of Behavior is accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>. Unless otherwise specified, the DHS Rules of Behavior shall be signed within thirty (30) days of contract award. Any new Contractor employees assigned to the contract shall also sign the DHS Rules of Behavior before accessing DHS systems and sensitive information. The Contractor shall maintain signed copies of the DHS Rules of Behavior for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, the Contractor shall e-mail copies of the signed DHS Rules of Behavior to the COR not later than thirty (30) days after contract award for each employee. The DHS Rules of Behavior will be reviewed annually, and the COR will provide notification when a review is required.

(c) *Privacy Training Requirements.* All Contractor and subcontractor employees that will have access to Personally Identifiable Information (PII) and/or Sensitive PII (SPII) are required to take *Privacy at DHS: Protecting Personal Information* before accessing PII and/or SPII. The training is accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>.

Training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall also complete the training before accessing PII and/or SPII. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Initial training certificates for each Contractor and subcontractor employee shall be provided to the COR not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

H.5. SAFEGUARDING OF SENSITIVE INFORMATION (MAR 2015)

(a) *Applicability.* This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as "Contractor"). The Contractor shall insert the substance of this clause in all subcontracts.

Section H

(b) *Definitions.* As used in this clause—

“Personally Identifiable Information (PII)” means information that can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, either alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-personally identifiable information can become personally identifiable information whenever additional information is made publicly available—in any medium and from any source—that, combined with other available information, could be used to identify an individual.

PII is a subset of sensitive information. Examples of PII include, but are not limited to: name, date of birth, mailing address, telephone number, Social Security number (SSN), email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), static Internet protocol addresses, biometric identifiers such as fingerprint, voiceprint, iris scan, photographic facial images, or any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual.

“Sensitive Information” is defined in HSAR clause 3052.204-71, Contractor Employee Access, as any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, “Policies and Procedures of Safeguarding and Control of SSI,” as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as “For Official Use Only,” which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to

Section H

the national or homeland security interest; and

(4) Any information that is designated “sensitive” or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

“Sensitive Information Incident” is an incident that includes the known, potential, or suspected exposure, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access or attempted access of any Government system, Contractor system, or sensitive information.

“Sensitive Personally Identifiable Information (SPII)” is a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements. Examples of such PII include: Social Security numbers (SSN), driver’s license or state identification number, Alien Registration Numbers (A-number), financial account number, and biometric identifiers such as fingerprint, voiceprint, or iris scan. Additional examples include any groupings of information that contain an individual’s name or other unique identifier plus one or more of the following elements:

- (1) Truncated SSN (such as last 4 digits)
- (2) Date of birth (month, day, and year)
- (3) Citizenship or immigration status
- (4) Ethnic or religious affiliation
- (5) Sexual orientation
- (6) Criminal History
- (7) Medical Information
- (8) System authentication information such as mother’s maiden name, account passwords or personal identification numbers (PIN)

Other PII may be “sensitive” depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII but is not sensitive.

(c) *Authorities.* The Contractor shall follow all current versions of Government policies and guidance accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>, or available upon request from the Contracting Officer, including but not limited to:

- (1) DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use Only) Information
- (2) DHS Sensitive Systems Policy Directive 4300A
- (3) DHS 4300A Sensitive Systems Handbook and Attachments
- (4) DHS Security Authorization Process Guide
- (5) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information
- (6) DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program

Section H

- (7) DHS Information Security Performance Plan (current fiscal year)
- (8) DHS Privacy Incident Handling Guidance
- (9) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at <http://csrc.nist.gov/groups/STM/cmvp/standards.html>
- (10) National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations accessible at <http://csrc.nist.gov/publications/PubsSPs.html>
- (11) NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at <http://csrc.nist.gov/publications/PubsSPs.html>

(d) *Handling of Sensitive Information.* Contractor compliance with this clause, as well as the policies and procedures described below, is required.

(1) Department of Homeland Security (DHS) policies and procedures on Contractor personnel security requirements are set forth in various Management Directives (MDs), Directives, and Instructions. *MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information* describes how Contractors must handle sensitive but unclassified information. DHS uses the term "FOR OFFICIAL USE ONLY" to identify sensitive but unclassified information that is not otherwise categorized by statute or regulation. Examples of sensitive information that are categorized by statute or regulation are PCII, SSI, etc. The *DHS Sensitive Systems Policy Directive 4300A* and the *DHS 4300A Sensitive Systems Handbook* provide the policies and procedures on security for Information Technology (IT) resources. The *DHS Handbook for Safeguarding Sensitive Personally Identifiable Information* provides guidelines to help safeguard SPII in both paper and electronic form. *DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program* establishes procedures, program responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.

(2) The Contractor shall not use or redistribute any sensitive information processed, stored, and/or transmitted by the Contractor except as specified in the contract.

(3) All Contractor employees with access to sensitive information shall execute *DHS Form 11000-6, Department of Homeland Security Non-Disclosure Agreement (NDA)*, as a condition of access to such information. The Contractor shall maintain signed copies of the NDA for all employees as a record of compliance. The Contractor shall provide copies of the signed NDA to the Contracting Officer's Representative (COR) no later than two (2) days after execution of the form.

(4) The Contractor's invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions shall not maintain SPII. It is acceptable to maintain in these systems the names, titles and contact information for the COR or other Government personnel associated with the administration of the contract, as needed.

(e) *Authority to Operate.* The Contractor shall not input, store, process, output, and/or transmit sensitive information within a Contractor IT system without an Authority to Operate (ATO) signed by the Headquarters or Component CIO, or designee, in consultation with the

Section H

Headquarters or Component Privacy Officer. Unless otherwise specified in the ATO letter, the ATO is valid for three (3) years. The Contractor shall adhere to current Government policies, procedures, and guidance for the Security Authorization (SA) process as defined below.

(1) Complete the Security Authorization process. The SA process shall proceed according to the *DHS Sensitive Systems Policy Directive 4300A* (Version 11.0, April 30, 2014), or any successor publication, *DHS 4300A Sensitive Systems Handbook* (Version 9.1, July 24, 2012), or any successor publication, and the *Security Authorization Process Guide* including templates.

(i) Security Authorization Process Documentation. SA documentation shall be developed using the Government provided Requirements Traceability Matrix and Government security documentation templates. SA documentation consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). During the development of SA documentation, the Contractor shall submit a signed SA package, validated by an independent third party, to the COR for acceptance by the Headquarters or Component CIO, or designee, at least thirty (30) days prior to the date of operation of the IT system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of a modified SA package. Once the ATO has been accepted by the Headquarters or Component CIO, or designee, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. The Government's acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the IT system controls are implemented and operating effectively.

(ii) Independent Assessment. Contractors shall have an independent third party validate the security and privacy controls in place for the system(s). The independent third party shall review and analyze the SA package, and report on technical, operational, and management level deficiencies as outlined in *NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations*. The Contractor shall address all deficiencies before submitting the SA package to the Government for acceptance.

(iii) Support the completion of the Privacy Threshold Analysis (PTA) as needed. As part of the SA process, the Contractor may be required to support the Government in the completion of the PTA. The requirement to complete a PTA is triggered by the creation, use, modification, upgrade, or disposition of a Contractor IT system that will store, maintain and use PII, and must be renewed at least every three (3) years. Upon review of the PTA, the DHS Privacy Office determines whether a Privacy Impact Assessment (PIA) and/or Privacy Act System of Records Notice (SORN), or modifications thereto, are required. The Contractor shall provide all support necessary to assist the Department in completing the PIA in a timely manner and shall ensure that project management plans and schedules include time for the completion of the PTA, PIA, and SORN (to the extent required) as milestones. Support in this context includes responding timely to requests for information from the Government about the use, access, storage, and maintenance of PII on the Contractor's system, and providing timely review of relevant compliance documents for