APPENDIX O – SDDOH SECURITY AND CONFIDENTIALITY PROGRAM REQUIREMENT CHECKLIST

Person completing form (please print): _____

Title: _____ Date: _____

Sign your name: _____

Program Area/Job Title: _____

Requirements (Initial items as completed)

___ Requirement 1: Policies must be in writing. (1.0)

___ Requirement 2: Policies must be readily accessible by any staff having access to confidential surveillance information or data at the central level and, if applicable, at noncentral sites. (1.1)

___ Requirement 3: A policy must name the individual who is the Overall Responsible Party (ORP) for the security system. (1.2)

___ Requirement 4: In compliance with CDC's cooperative agreement requirement, the ORP must certify annually that all program requirements are met. (1.2)

___ Requirement 5: A policy must clearly outline the roles of all individuals authorized to access specific types of information and establish the standard procedures or methods to be followed for staff outside the surveillance unit when access is deemed necessary. (1.3)

___ Requirement 6: A policy must describe methods for the review of security practices for HIV/AIDS surveillance data. Included in the policy should be a requirement for an ongoing review of evolving technology to ensure that data remain secure. (1.4)

___ Requirement 7: All authorized personnel with access to surveillance data are responsible for reporting any suspected security breaches. This requirement must also be included in the training provided to non-surveillance staff. (1.5)

___ Requirement 8: Any breach of confidentiality must be promptly investigated to determine the cause and implement appropriate corrective actions. (1.5)

___ Requirement 9: Any breach that leads to the disclosure of private information about one or more individuals (a breach of confidentiality) must be reported immediately to the Team Leader of the Reporting, Analysis, and Evaluation Team, HIV Incidence and Case Surveillance Branch, DHAP, NCHSTP, CDC. The CDC may provide support to the surveillance unit handling the incident. In coordination with appropriate legal counsel, surveillance staff should assess whether the breach should be reported to law enforcement agencies. (1.5)

___ Requirement 10: All individuals with access to surveillance data are required to complete annual security training. The date of their initial training must be recorded in their personnel file. IT staff and contractors who need access to data must complete the same training as surveillance personnel and sign the same confidentiality agreements. This requirement applies to anyone with access to servers, workstations, backup devices, or similar systems. (1.6)

___ Requirement 11: All authorized personnel are required to sign a confidentiality statement annually. Newly hired or newly authorized staff must sign this statement before being granted access to surveillance data. They must present the signed statement to the individual responsible for issuing passwords and keys prior to receiving access. The statement must affirm that the employee understands and agrees not to disclose surveillance data or information to anyone not authorized by the ORP. The original signed statement must be kept in the employee's personnel file. (1.7)

___ Requirement 12: Every member of the surveillance team and all individuals authorized to access case-specific information, as outlined in this document, must be well-informed about the organization's information security policies and procedures. Additionally, all authorized staff are responsible for questioning anyone who attempts to access surveillance data without proper authorization. (1.8)

__ Requirement 13: All authorized staff members are personally responsible for securing their workstations, laptops, or any other devices used to access confidential surveillance information or data. This includes safeguarding keys, passwords, and access codes that provide entry to sensitive information. Staff must also take precautions to prevent introducing computer viruses to surveillance software and avoid damaging hardware by exposing it to extreme temperatures. (1.8)

___ Requirement 14: Simultaneous access of SDEDSS and public internet websites should not occur. Care should be taken when using email applications (e.g. Outlook) and SDEDSS simultaneously to ensure sensitive or confidential information is not inadvertently transmitted. When using Outlook to communicate sensitive or confidential information, users must use secure email settings within Outlook. (1.8)

___ Requirement 15: Access to surveillance information containing names for research purposes (beyond routine surveillance) must be granted only when there is a demonstrated need for the names, Institutional Review Board (IRB) approval has been obtained, and a confidentiality statement outlining access rules and final disposition of the information has been signed. Access to surveillance data without names for research purposes outside of routine surveillance may also require IRB approval, depending on the number and type of variables requested, in accordance with local data release policies. (2.4)

___ Requirement 16: Access to confidential surveillance information and data by personnel outside the surveillance unit must be limited to those authorized based on an expressed and justifiable public health need, must not compromise or impede surveillance activities, must not affect the public perception of confidentiality of the surveillance system, and must be approved by the ORP. (3.1)

___ Requirement 17: Access to surveillance information with identifiers by those who maintain other disease data stores must be limited to those for whom the ORP has weighed the benefits and risks of allowing access and can certify that the level of security established is equivalent to the standards described in this document. (3.3)

___ Requirement 18: Access to surveillance information or data for nonpublic health purposes, such as litigation, discovery, or court order, must be granted only to the extent required by law. (3.4)

___ Requirement 19: Access to and uses of surveillance information or data must be defined in a data release policy. (3.8)

___ Requirement 20: A policy must incorporate provisions to protect against public access to raw data or data tables that include small denominator populations that could be indirectly identifying. (3.8)

___ Requirement 21: All physical locations containing electronic, or paper copies of surveillance data must be enclosed inside a locked, secured area with limited access. Workspace for individuals with access to surveillance information must also be within a secure locked area. Paper copies of surveillance information containing identifying information must be housed inside locked filed cabinets that are inside a locked room (4.1)

___ Requirement 22: Accessing SDEDSS during business travel, users must use the secure Citrix Application, be in a private secure room while working in SDEDSS. Users must log off SDEDSS and Citrix or lock the computer, when not present in the room. (4.1)

___ Requirement 23: Surveillance information with personal identifiers must not be taken to private residences unless specific documented permission is received from the ORP. (4.1)

___ Requirement 24: Prior approval must be obtained from the ORP when planned business travel precludes the return of surveillance information with personal identifiers to the secured area by the close of business on the same day. (4.1)

___ Requirement 25: Each member of the surveillance team must shred documents containing confidential information before disposing of them. Shredders should be of commercial quality with a crosscutting feature. (4.2)

___ Requirement 26: A policy must establish procedures for managing both incoming and outgoing mail within the surveillance unit. The volume and sensitivity of information included in each piece of mail should be minimized. (4.3)

___ Requirement 27: Rooms containing surveillance data must not be easily accessible by window. (4.3)

___ Requirement 28: Access to any secured areas that either contain surveillance data or can be used to access surveillance data by unauthorized individuals can only be granted during times when authorized surveillance or IT personnel are available for escort or under conditions where the data are protected by security measures specified in a written policy and approved by the ORP. (4.4)

___ Requirement 29: When identifying information is taken from secured areas and included on line lists or supporting notes, in either electronic or hard copy format, these documents must contain only the minimum amount of information necessary for completing a given task and, where possible, must be coded to disguise any information that could easily be associated with HIV(900), AIDS(950), Syphilis(700), GC (300) and Chlamydia (200). (4.5)

___ Requirement 30: Surveillance information must have personal identifiers removed (an analysis dataset) if taken out of the secured area or accessed from an unsecured area. (4.5)

___ Requirement 31: An analysis dataset must be held securely by using protective software (i.e., software that controls the storage, removal, and use of the data). (5.1)

___ Requirement 32: Data transfers and methods for data collection must be approved by the ORP and incorporate the use of access controls. Confidential surveillance data or information must be encrypted before electronic transfer. Ancillary databases or other electronic files used by surveillance also need to be encrypted when not in use. (5.2)

___ Requirement 33: When case-specific information is electronically transmitted, any transmission that does not incorporate the use of an encryption package meeting the Advanced Encryption Standard (AES) encryption standards and approved by the ORP must not contain identifying information or use terms easily associated with HIV/AIDS. The terms HIV or AIDS, or specific behavioral information must not appear anywhere in the context of the communication, including the sender and/or recipient address and label. (5.3)

___ Requirement 34: Laptops, tablets and other portable devices that receive or store surveillance information with personal identifiers must incorporate the use of encryption software. Surveillance information with identifiers must be encrypted and stored on an external storage device or on the laptop's removable hard drive. The external storage device or hard drive containing the data must be separated from the laptop and held securely when not in use. The decryption key must not be on the laptop. Other portable devices without removable or external storage components must employ the use of encryption software that meets federal standards. (5.4)

___ Requirement 35: Acceptable methods of sanitizing diskettes and other storage devices that previously contained sensitive data include overwriting or degaussing before reuse. If the machine is coming through surplus, it will be wiped/sanitized. If the machine is not coming through surplus and needs to be wiped, make request through the Help Desk asking that a 3-pass wipe of the hard drive be performed. (5.5)