Classified National Security Information Program for State, Local, Tribal and Private Sector Entities

Implementing Directive

February 2012

Homeland Security

Department of Homeland Security
Office of the Chief Security Officer
Washington, D.C. 20528

Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities Implementing Directive

Foreword

This directive is issued under the authority of Executive Order 13549, "Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities."

The need to share actionable, timely, and relevant classified information among Federal, State, Local, Tribal, and Private Sector (SLTPS) partners in support of homeland security is self-evident. Equally evident is the need for a unified, consistent program for the application of standardized security processes and procedures for security clearance management and the safeguarding of classified information across the executive branch and in support of classified information sharing efforts with our partners in the SLTPS communities. To address these needs, on August 18, 2010, the President issued Executive Order 13549.

Under the authority of the Order, and through this implementing directive, a governance and oversight structure are put in place that will serve to instill and promote the uniform application of security standards within the executive branch and SLTPS communities while maintaining consistency with existing policies and standards as promulgated through statutes, executive orders, regulations, and other directives. This directive, which represents the combined and collaborative efforts of stakeholders within the Federal and SLTPS communities, will serve to lay a consistent security foundation across the information sharing enterprise and thereby further enhance the confidence necessary to support the sharing of classified information.

Users of this directive are encouraged to bring forth any concerns or questions with the guidance provided herein and recommend any changes that might improve the program. Communications on the directive can be addressed to:

Department of Homeland Security
Office of the Chief Security Officer
State, Local, Tribal, and Private Sector Security Management Division
(SLTPS/SMD)
Washington D.C. 20528
Email: SLTPSSecurity@dhs.gov

Janet Napolitano
Secretary
Department of Homeland Security

Date: March 1, 2012

TABLE OF CONTENTS

APPENDICES AND FORMS

CHAPTER 1

General Provisions and Requirements

1-100. Purpose. This directive is issued in accordance with Executive Order 13549, "Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities."[1] Its purpose is to instill uniformity and consistency in the application of security standards for state, local, tribal and private sector entities (SLTPS[2]) with whom classified information is shared and prescribes the processes and standards for providing access to and safeguarding of such information when shared with SLTPS entities.

1-101. Authority.

a. The Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities, hereafter referred to as the SLTPS Program, was established by Executive Order (E.O.) 13549 to ensure that security standards governing access to and safeguarding of classified information shared with SLTPS entities are applied uniformly and consistently and in accordance with E.O. 13526 of December 29, 2009 ("Classified National Security Information"), E.O. 12968 of August 2, 1995, as amended ("Access to Classified Information"), E.O. 13467 of June 30, 2008 ("Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information"), and E.O. 12829 of January 6, 1993, as amended, ("National Industrial Security Program").

b. Pursuant to E.O. 13549., the National Security Advisor shall provide overall policy guidance for the SLTPS Program. The Secretary of Homeland Security is designated by the President as the Executive Agent (EA) for the SLTPS Program and shall implement and oversee its administration in consultation with the Director of the Information Security Oversight Office, the Director of the Office of Management and Budget, and the heads of affected agencies.

c. Further, the Secretary of Homeland Security is directed, pursuant to P.L. 111-258, "Reducing Over-Classification Act," to designate a "Classified Information Advisory Officer," who shall develop and administer training programs to assist SLTPS in developing plans and policies for communicating sensitive unclassified information[3] to individuals who lack the appropriate security clearance, procedures for challenging the classification of information, and the means by which SLTPS personnel may apply for a security clearance.

---

[1] As indicated in Appendix 9, Section EE, of this directive, "State" also includes U.S. Territories and the District of Columbia.

[2] Throughout this directive, when referring to state, local, tribal, and private sector collectively the acronym is SLTPS. Where the acronym SLT is used alone it refers only to state, local and tribal. Where the acronym PS is used alone it refers only to private sector.

[3] Pursuant to Executive Order 13556, "Controlled Unclassified Information (CUI)," and in accordance with implementing directives and implementation timelines to be issued by the CUI Executive Agent, CUI and its associated categories and subcategories will become, on a specific date yet to be determined, the exclusive designation for identifying unclassified information of a sensitive nature.

d. Nothing in this directive shall be construed to supersede or change the authorities of the Secretary of Energy or the Nuclear Regulatory Commission under the Atomic Energy Act of 1954, as amended (42 U.S.C. 2011 et seq.); the Secretary of Defense under E.O. 12829, as amended; the Director of the Information Security Oversight Office under E.O. 13526 and E.O. 12829, as amended; the Attorney General under title 18 United States Code and the Foreign Intelligence Surveillance Act (50 U.S.C. 1801 et seq.); the Secretary of State under title 22, United States Code, and the Omnibus Diplomatic Security and Antiterrorism Act of 1986; or the Director of National Intelligence under the National Security Act of 1947, as amended, E.O. 12333, as amended, E.O. 12968, as amended, E.O. 13467, and E.O. 13526.

1-102. Scope.

a. This directive is applicable to all SLTPS personnel who have been sponsored for or granted a security clearance for access to classified information by a Federal agency under the SLTPS Program and each Federal agency that has or will sponsor an SLTPS individual for a security clearance and access to classified information. This directive is not applicable to PS personnel who have or will be granted a security clearance based on their employment or association with a company or other commercial entity that falls under the purview of E.O. 12829 and the National Industrial Security Program Operating Manual (NISPOM).

b. This directive is applicable to all SLT facilities owned or operated by an SLT entity where classified information is or will be physically stored, regardless of the media. Pursuant to E.O. 12829, as amended, the Secretary of Defense, or the cognizant security agency, shall provide program management, oversight, inspection, accreditation and monitoring of all PS facilities that physically store classified information.

c. Only to the extent that an action is not otherwise governed under E.O. 12829 and the NISPOM, this directive is also applicable to contractors, licensees, grantees and certificate holders performing on or who seek to perform on a contract or other legally binding instrument originated by and under the exclusive management and control of an SLT entity and whereby access to classified information by the contractor, licensee, grantee, or certificate holder is required in performance of the effort (See Chapter 8, Contracting for Classified Support). This directive shall only be applicable relative to the process and procedures for establishing a legally binding connection between the SLT entity, the contractor, and the Federal government that will allow the SLT entity to contract for classified support and the contractor to access classified information under the terms of the contract and under the cognizance of the National Industrial Security Program (NISP).

1-103. Responsibilities.

a. The Secretary of Homeland Security, as EA for the SLTPS Program, shall be responsible for:

(1) overall program management and oversight;

(2) accreditation, monitoring, and periodic inspection of all facilities owned or operated by SLT entities that have access to classified information, except when another agency has entered into an agreement with the Department of Homeland Security (DHS) to perform some or all of these functions;

(3) processing of security clearance applications by SLTPS personnel that are sponsored by DHS and, when requested by a sponsoring agency, processing the applications of the requesting sponsoring agency on a reimbursable basis unless otherwise determined by DHS and the sponsoring agency.

(4) documenting and tracking the final status of security clearances for all SLTPS personnel in consultation with the Office of Personnel Management (OPM), the Department of Defense (DOD), and the Office of the Director of National Intelligence (ODNI);

(5) developing and maintaining a security profile of SLT facilities that have access to classified information and making available to other agencies such information, upon request and as appropriate;

(6) developing training, in consultation with the SLTPS Policy Advisory Committee, for all SLTPS personnel who have been determined eligible for access to classified information, which shall cover the proper safeguarding of classified information and sanctions for unauthorized disclosure of classified information;

(7) issuing and maintaining this directive in consultation with affected executive departments and agencies, and with the concurrence of the Secretary of Defense, the Attorney General, the Director of National Intelligence, and the Director of the Information Security Oversight Office; and,

(8) designating an official to serve as the "Classified Information Advisory Officer" (CIAO), pursuant to P.L. 111-258, and notifying the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives, of the designation.

b. The head of each Federal agency that shares classified information with SLTPS entities shall:

(1) designate a senior official to direct and administer the agency's implementation and compliance with the SLTPS Program and provide designee contact information to the DHS, SLTPS Security Management Division (DHS SLTPS/SMD);

(2) ensure that agency implementing regulations, internal rules, and/or guidelines are consistent with this directive and updated as necessary;

(3) ensure that they or their designated senior official takes appropriate and prompt corrective action whenever a violation of this directive occurs;

(4) account each year for the costs within the agency associated with the implementation of this program. These costs shall be reported as directed by the Director of the Information Security Oversight Office (ISOO); and

(5) provide DHS SLTPS/SMD with applicable security clearance and other appropriate security records associated with SLTPS personnel and facilities. Such records shall be provided in a manner determined by the Secretary of Homeland Security or his/her designee.

c. SLTPS personnel with whom classified information is shared shall:

(1) safeguard all classified information to which they have knowledge or access in accordance with this directive and other applicable governing orders, regulations, and directives;

(2) execute agreements as cited in Section 3-101.e. of this directive, with DHS or other appropriate Federal agency, as applicable and in accordance with this directive, for the safeguarding of classified information stored at an SLT owned or operated facility and the acquisition and oversight of contractor services procured in support of a contract that includes access to classified information by contractor employees;

(3) complete security training as required by this directive; and,

(4) pursuant to Chapter 7 of this directive, immediately report any incident where classified information has been possibly compromised or disclosed to an unauthorized person.

1-104. Security Cognizance.

a. Each Federal agency that sponsors an SLTPS individual for the issuance of a security clearance and access to classified information shall maintain security cognizance over the individual in accordance with its respective procedures, to include application processing, investigation, adjudication, execution of a classified information non-disclosure agreement, training, continuing evaluation, and the determination of need-to-know requirements pursuant to E.O. 13526 and its implementing directives. An agency may transfer security cognizance to DHS upon execution of a written agreement between the agency and DHS. Such transfers shall be on a reimbursable basis unless determined otherwise by DHS and the applicable agency. Refer to Chapter 2, Personnel Security Clearances, for additional guidance.

b. DHS shall assume security cognizance of all SLT owned or operated facilities where classified information is stored; this cognizance shall include accreditation, monitoring, and periodic inspection. An agency may retain security cognizance over such facilities that are under its exclusive sponsorship upon execution of a written agreement between the agency and DHS. Refer to Chapter 3, Physical Security, for additional guidance.

1-105. Control of Information.

a. Pursuant to section 892(e) of the Homeland Security Act of 2002 (6 U.S.C. 482(e)), as amended, all information provided to an SLTPS entity from a Federal agency shall remain under the control of the Federal Government. Any state or local law authorizing or requiring disclosure shall not apply to such information.

b. Information that is classified pursuant to E.O. 13526 or its predecessor or successor orders is the property of the U.S. Government and shall remain under the control of the Federal Government.

1-106. State, Local, Tribal, and Private Sector Policy Advisory Committee.

a. The SLTPS Policy Advisory Committee (Committee) is established as a forum to discuss SLTPS Program-related policy issues and make recommendations regarding the content of this directive; consult on proposed changes to policies and procedures that will remove undue impediments to information sharing; and facilitate the resolution of disputes on matters governed by this directive.

b. The Committee shall be comprised of the following members: The Director, ISOO, who shall serve as Chair of the Committee; a DHS official designated by the Secretary of Homeland Security and a representative of SLTPS entities, who shall serve as Vice Chairs of the Committee; and representatives designated by the heads of the Departments of State, Defense, Justice, Transportation and Energy, the Nuclear Regulatory Commission (NRC), ODNI, the Central Intelligence Agency (CIA), and the Federal Bureau of Investigation (FBI). Additional members representing other agencies or SLTPS entities are appointed based on nomination by any Committee member and approval by the Chair.

c. The Committee is subject to the Federal Advisory Committee Act (FACA), the Freedom of Information Act (FOIA), and the Government in the Sunshine Act (GISA), and shall function in accordance with the charter and by-laws established as required for such Committees.

1-107. Directive Interpretations. All requests for interpretations of this directive, as well as questions, concerns, complaints, or other issues related to the Program, may be addressed to:

Department of Homeland Security
Office of the Chief Security Officer
State, Local, Tribal, and Private Sector Security Management Division (SLTPS/SMD)
Washington D.C. 20528

Email: SLTPSSecurity@dhs.gov

1-108. Waivers to this Directive.

a. SLTPS requests for waivers specific to the requirements cited in this directive and that are not governed by other orders, directives or regulations, shall be submitted through the applicable Federal agency sponsor to DHS SLTPS/SMD. The request shall specify in writing the reason why it is impractical or unreasonable to comply with the applicable requirement, the proposed duration for the waiver to remain in force, and appropriate alternative measures to achieve the same result as stipulated in this directive.

b. Federal agency requests for waivers specific to the requirements cited in this directive and that are not governed by other orders, directives or regulations, shall be submitted directly from the agency to the DHS SLTPS/SMD. The request shall specify in writing the reason why it is impractical or unreasonable to comply with the applicable requirement, the proposed duration for the waiver to remain in force, and appropriate alternative measures to achieve the same result as stipulated in this directive.

c. Where a waiver has a direct impact or association with the equities of other Federal agencies, DHS SLTPS/SMD shall coordinate approval of the waiver with the affected agencies.

d. Waivers from requirements governed by other orders, regulations or directives shall be processed in the manner prescribed by the applicable order, regulation, or directive. When such waivers affect the SLTPS Program as prescribed in this directive, the applicable agency shall first coordinate with DHS SLTPS/SMD.

1-109. Conflict Resolution.

a. Federal agencies that share classified information with SLTPS entities shall ensure that security processes and procedures prescribed in this directive and other applicable executive orders and regulations are applied to SLTPS entities in a uniform and consistent manner.

b. Any conflict arising between this directive and other orders, regulations, or directives, shall be resolved at the lowest level possible. Where resolution at a lower level is not possible it shall be referred to the DHS SLTPS/SMD, and if necessary and applicable, the CIAO, or the State, Local, Tribal, and Private Sector Policy Advisory Committee (PAC), which, pursuant to E.O. 13549, may act towards facilitating a resolution. If the matter cannot be resolved through the CIAO or the SLTPS PAC it shall be presented to the National Security Advisor or designee, for a final determination. Pending resolution of the conflict, the order, regulation, or directive with the most restrictive requirement shall be followed.

1-110. Security Liaison (SL). The senior-most SLT official with management and operational authority over each SLT owned or operated facility where classified information is or will be stored shall appoint, in writing, an SL. A copy of the SL appointment letter shall be provided to DHS SLTPS/SMD. The SL shall possess a security clearance at least equal to the level of classified information stored at the facility. The SL shall oversee and direct security measures necessary for implementing applicable requirements of this directive and related Federal requirements for classified information and shall complete security training as specified in Chapter 6, Security Training. Refer to Appendix 1, State, Local, Tribal Security Liaison Duties and Responsibilities, for a synopsis of SL responsibilities.

CHAPTER 2

Personnel Security Clearances

2-101. General.

a. Personnel Security Clearances (PCL) for SLTPS personnel shall be issued in accordance with this directive and consistent with the policies and procedures established pursuant to E.O. 12968, as amended, E.O. 13467, and Intelligence Community Directive (ICD) 704, "Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information," as applicable, and their implementing directives.

b. A PCL and subsequent eligibility to access classified information is dependent upon the prior execution of a Standard Form (SF) 312, "Classified Information Non-disclosure Agreement," or other approved non-disclosure agreement prescribed by ISOO or the Director of National Intelligence (DNI).

c. SLTPS personnel who are granted a security clearance shall comply with all reporting requirements and associated responsibilities that accompany the granting of access to classified information as required by statute, order, or regulation, and, the sponsoring Federal agency.

d. PCLs issued to SLTPS personnel shall be reciprocally accepted by all agencies and SLTPS entities.

e. PCLs may be issued to SLTPS personnel when the write-for-release principle that allows for the sanitization of classified information to the sensitive but unclassified level is inadequate to satisfy the effective integration of SLTPS personnel into a singular effort to protect the homeland. Those personnel selected for the granting of a security clearance shall have a demonstrated and foreseeable need for access to classified information and be in a position to capitalize on the value the classified information provides. In determining the need for the granting of a security clearance the following criteria shall apply:

1. The granting of security clearances shall be kept to the minimum necessary in support of mission activities where access to classified information by SLTPS personnel is essential to the national security.

2. Agencies shall take into consideration that pursuant to Executive Order 13526, under exigent circumstances classified information may be released by designated Federal officials to personnel who are not otherwise cleared for access. Therefore, the granting of a security clearance strictly in support of potential contingencies is not necessarily justified or warranted.

3. Security clearances shall not exceed the Secret level except in those situations where there is a demonstrated and foreseeable need and the person being considered for a higher level security clearance will perform a function as cited below.

(a) Top Secret security clearances may be granted on a case by case basis, when the person to whom the clearance is to be granted is officially designated and appointed as the State Homeland Security Advisor (HSA), or, the person will be an active and continuing participant in

or member of a Federally sponsored board, committee, working group, task force, operations center, or other entity where the integration of SLTPS personnel is essential and participation or membership requires or will require access to Top Secret information, or, the sponsoring agency determines that a person has a particular expertise or role whereby there is a demonstrated and foreseeable need for access to Top Secret information. The granting of such clearances shall be in accordance with and under the purview of Executive Order 12968, as amended, "Access to Classified Information."

(b) Access to Sensitive Compartmented Information (SCI) may be granted on a case by case basis, when the person to whom the access is to be granted is or will be an active and continuing participant in or member of a Federally sponsored board, committee, working group, task force, operations center, or other entity where the integration of SLTPS personnel is essential and participation or membership requires or will require access to SCI, or, the sponsoring agency determines that a person has a particular expertise or role whereby there is a demonstrated and foreseeable need for access to SCI. In determining the appropriateness of granting SCI access, significant consideration shall be given to the value such access will bring to the effort for which the individual will participate, the contributions that can be made by the individual in support of the effort, and the fact that the use of the information to which access is granted is strictly limited to within the Federally sponsored effort. Access to SCI shall only be provided in an appropriately accredited SCI Facility (SCIF) under the direct control of DHS or another Federal agency. Under no circumstances shall SCI material be released to the physical custody of SLTPS personnel outside of an approved SCIF. The granting of such access shall be in accordance with and under the purview of ICD 704, and/or subsequent guidance issued by the DNI.

(c) Prior to submitting a request for a Top Secret PCL and/or SCI access, consideration shall be given to the length of time it takes between the time a background investigation is requested and the time a security clearance can be issued to ensure the individual subjected to the investigation will still be available for the assignment and valuable investigative and financial resources are not wasted. As such, prior to processing for a security clearance, agencies should ensure that the individual is committed to continued active participation in the specific activity for a period of no less than one year after being granted the security clearance.

4. Absent disqualifying conduct as determined by the clearance granting official and upon the execution of a non-disclosure agreement prescribed by ISOO or the DNI, a duly elected or appointed governor, or the single most senior government official of a State, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, or an official who has succeeded to that office under applicable law, may be granted access to classified information in support of a counter-terrorism or homeland security mission without a background investigation. This authorization of access may not be further delegated to any other person and is applicable to no other SLTPS personnel.

(a) DHS shall maintain a central repository for the maintenance and retention of non-disclosure agreements executed by a governor or the single most senior government official with the exception of those agreements required pursuant to access to SCI or other special access program information. In the latter instances, the sponsoring Federal agency shall retain the

applicable agreement unless they have transferred personnel security responsibilities to DHS in accordance with Section 2-103 of this directive.

(b) Disqualifying conduct refers to any conduct that calls into question the reliability and trustworthiness of the individual to safeguard classified information in accordance with E.O. 12968, as amended, and the Adjudicative Guidelines for Determining Eligibility for Access to Classified Information.

(c) Access to classified information is not a right and is not absolute but is based on a need for access to such information in order to act on or otherwise fulfill an authorized governmental function associated with national security. An agency may exclude an individual from access to certain classified information to which they may otherwise be eligible when the information would provide insight into an investigation or other activity that may have a direct or indirect connection to the governor, or the single most senior government official, or the functions performed by that office.

5. Security clearances for SLTPS personnel shall be limited to U.S. citizens only.

2-102. SLTPS Positions Eligible for a Security Clearance.

a. SLT personnel who may be considered for a security clearance include the following:

1. Senior homeland security personnel, such as homeland security and emergency management coordinators, senior law enforcement personnel, senior public health officials, and other senior personnel who are responsible to advise the governor on homeland security issues.

2. For city, municipal and county governments and other political subdivisions of a State or territory of the United States, including the mayor of the District of Columbia: a mayor, county executive, city manager, senior law enforcement officer, senior firefighter, senior public health official, emergency manager or other senior government official employed by a city, municipality or county or other political subdivision of a State or territory of the United States involved in furthering United States homeland security.

3. Other law enforcement, public health and first responder officials participating in a Federally sponsored or endorsed board, committee, working group, task force, operations center, Fusion Center, or similar entity where access to classified information is required, as determined by the sponsoring Federal agency, may be considered for a security clearance.

b. PS personnel who do not fall under the purview of Executive Order 12829, "National Industrial Security Program," shall be processed for access eligibility in the same manner as SLT personnel. The granting of a security clearance to PS personnel shall be limited to the minimum number necessary to support the protection of critical infrastructure and security of the homeland.

1. Eligibility for a security clearance for PS personnel under the SLTPS Program does not apply to any corporation, company, contractor, licensee, grantee, individual or other commercial entity, or their subcontractors, that has entered into or seeks to enter into a contractual arrangement or consulting agreement with an agency of the Federal government pursuant to E.O. 12829, as

amended; or, any corporation, company, contractor, licensee, grantee, individual or other commercial entity, or their subcontractors, that is eligible for the granting of a facility security clearance under the authority of E.O. 12829, as amended, except when uncleared PS personnel are not associated with such arrangement or agreement and therefore not eligible for a security clearance under E.O. 12829, as amended.

2. PSCs may be issued to those personnel who have a demonstrated and foreseeable need for access to classified information; are in leadership, managerial or executive level positions; and are in a position to capitalize on the value of the classified information shared. Examples of such personnel include: leadership personnel (e.g., Sector Coordinating Council, Information Sharing and Analysis Centers as identified by their Sector Coordinating Council as the Sector's Information Sharing mechanism), who have the authority and stature to influence critical infrastructure and key resources (CIKR) owners/operators and others throughout the sector to take action; CIKR owners and operators (e.g., senior company executives including corporate security officers) of critical systems/assets/functions/networks that have been identified by DHS as critical infrastructure, including Level 1 and Level 2 facilities; subject matter experts who have been identified and selected to assist Federal and State CIKR agencies to interpret operational information and translate intelligence information into actionable information for CIKR owners and operators and government officials; and PS personnel who are nominated to serve on boards, commissions, committees or other Federally sponsored groups where access to classified information is required in order to participate in and carry out the functions of the group.

(a) PS personnel to whom a security clearance is issued under the SLTPS Program shall execute a "Statement of Understanding Relative to the Protection of Classified National Security Information." The purpose of the form is to inform and impress upon the signatory that the protection of classified information takes precedence over corporate loyalty and influence. As such they are legally obligated to abide by Federal standards for the safeguarding of and access to classified information and must resist and report any undue influence on the part of uncleared personnel, regardless of their position, to gain knowledge of classified information to which the signatory has been given access.

(b) DHS SLTPS/SMD, or the sponsoring Federal agency, shall maintain the original executed form in the PS individual's personnel security folder and/or the electronic equivalent.

2-103. Processing SLTPS Security Clearances.

a. Determining eligibility for access to classified information, and the funding, processing, maintenance, and management of SLTPS personnel security clearances is the responsibility of the sponsoring Federal agency unless an agency elects to transfer such responsibility to DHS.

1. If an agency elects to transfer responsibility for its SLTPS security clearance program to DHS, the applicable agency and DHS shall enter into a formal written agreement that outlines the details of the transfer and defines responsibilities. The agreement shall be executed by the applicable agency head or designee and the Secretary of Homeland Security or designee.

2. The transfer of SLTPS personnel security program responsibilities from another agency to DHS shall be on a reimbursable basis unless negotiated otherwise and codified in the agreement.

b. SLTPS personnel who are processed for a security clearance shall undergo the same investigative and adjudicative scrutiny as their Federal counterparts. No additional administrative or investigatory requirement shall be levied upon an SLTPS individual that is not applicable to other personnel to whom an equivalent level of access and security clearance is granted.

c. Each agency that retains responsibility for the processing, maintenance and management of SLTPS security clearances shall ensure that such processes are transparent and readily available to the SLTPS community. At a minimum, each agency shall provide to, and DHS SLTPS/SMD shall maintain, a catalog of agency processes available for review by the SLTPS community from one central location.

2-104. Documenting and Tracking SLTPS Security Clearances.

a. DHS shall, in consultation with OPM, DOD, and ODNI, develop a mechanism to document and track security clearance data on SLTPS personnel.

1. The mechanism developed shall allow for a central repository for all security clearances granted to SLTPS personnel but may exclude specific information on the reason(s) behind an action, such as a denial or revocation. The mechanism shall be accessible to those who have a need for its use and in accordance with security and privacy restrictions.

2. All agencies that grant security clearances to SLTPS personnel shall, either electronically or by other means, transfer, link, or otherwise input applicable security clearance data into the central repository. Excluded from this requirement is data on specific individuals when the disclosure of the association of a specific individual with an intelligence or law enforcement agency must be protected in the interest of national security, as determined by the intelligence or law enforcement agency.

b. To the extent practicable, the mechanism developed shall leverage an existing automated security clearance database system, such as the OPM Central Verification System (CVS).

c. Any costs associated with systems or software modifications to meet the central repository requirements outlined in this directive shall be borne by the system's owning agency unless costs are addressed through other arrangements.

CHAPTER 3

Physical Security

3-101. General.

a. When the sharing of classified information with SLT involves the on-site physical custody of classified information by an SLT entity at an SLT owned or operated facility, the location and manner in which classified information is to be stored and maintained shall meet all applicable physical and administrative security standards consistent with E.O. 13526, "Classified National Security Information," its implementing Directive, 32 C.F.R. Part 2001, and this directive.

b. SLTPS requests for waivers specific to the physical security standards cited in this directive shall be submitted to DHS SLTPS/SMD or the delegated Federal agency as cited in Section 3-101.d. below. The request shall specify in writing the reason why it is impractical or unreasonable to comply with the applicable requirement, the proposed duration for the waiver to remain in force, and appropriate alternative measures to achieve the same result as stipulated in this directive. Where a waiver has a direct impact or association with the equities of another Federal agency(ies), DHS SLTPS/SMD or a delegated Federal agency, as applicable, shall coordinate approval of the waiver with the affected agency(ies). Waivers from requirements governed by other orders, regulations or directives shall be processed in the manner prescribed by the applicable order, regulation, or directive. When such waivers affect the SLTPS Program as cited in this directive, the applicable agency shall first coordinate with DHS SLTPS/SMD.

c. On-site physical custody (storage) of classified information by SLT entities at an SLT owned or operated facility, to include the deployment of classified IT capabilities, as well as the use of secure communications (Secure Telephone Equipment/STE) and secure fax, shall be kept to the minimum necessary consistent with mission needs and shall not exceed the collateral Secret level. Exceptions to this limitation may be granted on a case-by-case basis when approved by an agency head or designee and the SLT facility (room/area) is under the full-time management, control, and operation of DHS or the sponsoring Federal agency - under no circumstances shall a SCIF be approved for, managed by, or placed under the control of an SLT entity.

d. SLT facilities where classified information is or will be stored shall be inspected, certified and undergo routine security oversight by DHS unless a sponsoring Federal agency has entered into an agreement with DHS to retain responsibility for this function. A sponsoring Federal agency that enters into such an agreement shall be referred to as the delegated Federal agency. As a delegated Federal agency it shall be authorized to perform defined security inspection, certification, accreditation, and oversight functions for those SLT owned or operated facilities it has sponsored.

1. If an agency chooses to retain responsibility for inspection, certification, accreditation, and oversight of SLT owned or operated facilities where classified information is or will be stored and for which it is the primary Federal sponsor, the applicable agency and DHS shall enter into a formal written agreement that outlines the details of the transfer and defines responsibilities. The agreement shall be executed by the applicable agency head or designee and the Secretary of Homeland Security or designee.

2. The application of security standards for the construction and operation of an SLT owned or operated facility shall be uniform and consistent with E.O. 13526, 32 C.F.R. Part 2001, and this directive.

3. Certification and accreditation of an SLT owned or operated facility for the storage of classified information by one agency shall be reciprocally accepted by all agencies unless the certification/accreditation is accompanied by a waiver. If a waiver has been issued, it is at the discretion of an agency as to whether or not to accept certification/accreditation.

4. If an agency enters into an agreement with DHS to retain responsibility for SLT owned or operated facilities for which it serves as the primary sponsor, the delegated agency shall provide DHS SLTPS/SMD with all necessary certification/accreditation data relative to the facility for inclusion in a centralized SLT Facility Security Profile database. Excluded from this requirement is data on specific facilities when the disclosure of the association of the specific facility with an intelligence or law enforcement agency must be protected in the interest of national security, as determined by the intelligence or law enforcement agency.

e. The senior-most SLT official with management and operational authority over each SLT owned or operated facility where classified information is or will be stored shall enter into a security agreement with DHS, or the delegated Federal agency, as applicable.

1. The agreement, "Security Agreement Between the U.S. Government and Non-U.S. Government Entities On The Safeguarding Of Classified National Security Information," shall be executed prior to certification/accreditation of the facility.

2. SLT owned or operated facilities that were approved for classified storage prior to publication of this directive shall execute the agreement with DHS, or the sponsoring Federal agency, within 120 days of this directive's publication.

3. DHS shall maintain a central repository of all executed agreements. A copy of the agreement executed between an SLT entity and another Federal agency shall be submitted to DHS SLTPS/SMD by the other Federal agency.

4. Where state, local, or tribal law preclude or prohibit the official cited in Section 3-101.e. above from entering into such an agreement, the agreement will be executed between DHS or the delegated Federal agency and the official authorized under the applicable state, local, or tribal law.

f. On-site physical storage of classified information by PS entities shall fall under the purview of E.O. 12829, "National Industrial Security Program" (NISP), and the NISPOM.

3-102. Deployment of Secure Telephone Equipment (STE) To Uncleared Private Sector Facilities.

a. The deployment of Secure Telephone Equipment (STE) and associated encryption devices does not constitute on-site physical storage of classified information. As such, a STE and associated encryption devices may be deployed to a PS facility that is not cleared under the purview of the NISP. In such instances, the following conditions shall be met:

1. The sponsoring agency head or designee has determined that it intends to share classified information with the intended recipient and that it is essential the intended recipient be provided with a classified communication capability to accommodate the need.

2. The device shall be encrypted to operate at no higher than the collateral Secret level.

3. DHS or the delegated Federal agency shall execute a written assessment regarding the risk of deploying a device at the PS facility, to include a determination on the existence of foreign ownership at any level within the corporate structure. If there is foreign ownership, DHS or the delegated Federal agency shall, in accordance with the National Security Agency (NSA) Policy Manual 3-16, "Control of Communications Security (COMSEC) Material," request a determination from the NSA Information Assurance Directorate, on the acceptability of deploying a STE and the associated encrypting device at the uncleared PS facility.

4. The PS individual to whom the device will be assigned has been issued a minimum of a final Secret security clearance and has executed a "Statement of Understanding Relative to the Protection of Classified National Security Information."

5. DHS or the delegated Federal agency determines that the room in which the device will be deployed meets or exceeds the requirements cited in Section 3-103.b.2. The "Multi-Use Security Survey Form for State, Local, Tribal, and Private Sector Programs" (Appendix 2) shall be used to conduct and record the survey results.

6. The associated encryption device shall be stored and maintained separate from the STE when not in use by the individual to whom it is assigned.

7. The authorized user of the STE and associated encryption device at an uncleared PS facility shall not take notes of any classified information conveyed when using the STE as the notes would constitute on-site physical storage of classified information and only PS facilities cleared under the auspices of the NISP may be authorized for on-site physical storage. As such, the requirement for the presence of equipment authorized for the destruction of classified information, as stipulated in section 3-103.b.2.(c) of this directive, does not apply.

b. A STE deployed at an uncleared PS facility under this program shall not be connected to or otherwise configured to send or receive documents through a facsimile (fax) machine or any other equipment that allows for the printing or electronic transfer of information. Doing so would constitute on-site physical storage of classified information and only PS facilities cleared under the auspices of the NISP may be authorized for on-site physical storage.

3-103. Criteria for Storage of Classified Information.

a. In all cases, the storage of classified information in any form at an SLT facility shall be based on the sponsorship and affirmation by a Federal agency of its intention to share classified information directly with the applicable SLT entity and the SLT persons with whom the classified information will be shared have been granted the appropriate level security clearance.

b. SLT facilities shall meet the following general standards for storage of any media that contains classified information.

1. On-Site Closed Storage of Confidential or Secret Information:

   (a) Verification and documentation by DHS SLTPS/SMD or the delegated Federal agency of the presence of a GSA-approved security container located in a private office.

   (b) Verification and documentation by DHS SLTPS/SMD or the delegated Federal agency of the presence of an NSA Approved High Security Cross Cut Shredder or other appropriate destruction equipment as cited in Section 4-107 of this directive.

   (c) DHS SLTPS/SMD or delegated Federal agency certification/accreditation that the environment in which classified information is stored meets the applicable security standards.

   (d) The "Multi-Use Security Survey Form for State, Local, Tribal, and Private Sector Programs" (Appendix 2) shall be used by DHS SLTPS/SMD or the delegated Federal agency to conduct and record the survey results.

2. STE with or without Secure Fax Capability:

   (a) Verification and documentation by DHS SLTPS/SMD or the delegated Federal agency that the phone is situated in a private office and that its installation meets appropriate COMSEC standards.

   (b) Verification and documentation by DHS SLTPS/SMD or the delegated Federal agency of the presence of a GSA-approved security container located in a private office.

   (c) Verification and documentation by DHS SLTPS/SMD or the delegated Federal agency of the presence of an NSA Approved High Security Cross Cut Shredder or other appropriate destruction equipment as cited in Section 4-107 of this directive.

   (d) DHS SLTPS/SMD or delegated Federal agency certification/accreditation that the environment in which classified capability is to be deployed meets the appropriate security standards.

   (e) The "Multi-Use Security Survey Form for State, Local, Tribal, and Private Sector Programs" (Appendix 2) shall be used by DHS SLTPS/SMD or the delegated Federal agency to conduct and record the survey results.

3. Secure Video Teleconferencing (SVTC):

   (a) Verification and documentation by DHS SLTPS/SMD or the delegated Federal agency of the presence of a GSA-approved security container located within the room/area.

   (b) Verification and documentation by DHS SLTPS/SMD or the delegated Federal agency of the presence of an NSA Approved High Security Cross Cut Shredder or other appropriate destruction equipment as cited in Section 4-107 of this directive.

(c) DHS SLTPS/SMD or delegated Federal agency certification/accreditation that the room/area in which the equipment will be deployed meets or exceeds construction and sound attenuation standards for the open storage of classified information as cited in Appendix 3, "State, Local, and Tribal Security Construction Standard for Open Storage Areas." The "SLT Open Storage Survey Checklist" (Appendix 4) shall be used by DHS SLTPS/SMD or the delegated Federal agency to conduct and record the survey results.

(d) Specific SVTC configurations may be approved in a closed storage environment when the associated classified equipment and keying material can be secured in a GSA approved security container when not in use, and, when the room meets the appropriate sound attenuation standards. Refer to Section VI of Appendix 3. In this instance the "SLT Closed Storage SVTC Processing Area Survey" (Appendix 5) shall be used to conduct and record the survey results.

(e) Verification and approval by DHS SLTPS/SMD or the delegated Federal agency of a Standard Operating Procedure (SOP) specific to the location, personnel, and facility and the operational environment of the room/area to be certified.

4. Classified Information Technology (IT) Systems**:** Systems and related technologies facilitate rapid and secure access and dissemination of time sensitive, actionable information. These systems also provide platforms for the integration, exchange, and analysis of information to detect, prevent, disrupt, preempt, and mitigate the effects of terrorist activity. When the dissemination, exchange and analysis of classified information is necessary and appropriate and where a classified IT system at a Federally controlled facility is unrealistic or is an impediment to the timely flow and analysis of information, the deployment of a classified IT system by a Federal agency to and under the physical control of an SLT entity may be warranted.

(a) Deployment of classified IT system by a Federal agency for use by but under the physical control of and at a facility owned or operated by an SLT entity shall not exceed the Secret level. IT systems refers to any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. This includes computers, ancillary equipment, software, still images, motion pictures, multimedia presentations, and related resources.

(b) Classified information shall not in any manner be entered into or processed on any IT system, to include stand-alone computers or laptops and personal electronic devices (PEDs), that have not been certified and accredited specifically for classified processing at the appropriate classification level by a Federal agency.

(c) The Homeland Secure Data Network (HSDN) shall be the U.S. Government's primary non-defense, Secret level classified information network, and where appropriate shall be deployed to SLT entities for use by appropriately cleared SLT personnel.

(d) Although HSDN is designed to be the primary non-defense U.S. Government classified network deployed to SLT entities, in some instances the Department of Defense (DOD) or another Federal agency may allow for or sponsor SLT activities for

access to its agency owned classified systems. In these instances the following criteria shall apply:

(1) Deployment of and access to the DOD owned and operated Secret Internet Protocol Router Network (SIPRNET), or any other Federal agency owned Secret level system, by SLT personnel shall be at the discretion of DOD or the appropriate Federal agency, as applicable, and in accordance with its respective requirements. In such cases the sponsoring Federal entity shall bear responsibility for all support functions, to include certification and accreditation of the system and supplying the appropriate cryptographic equipment.

(2) Access to the DOD owned SIPRNET or any other Federal agency system through the HSDN gateway by SLT personnel shall be at the discretion of DOD or the applicable Federal agency. Such requests shall be justified and supported by a Federal sponsor and submitted through the appropriate HSDN governing body to the applicable Federal agency for approval.

(3) Access to individual restricted portals and communities of interest resident in a classified network shall be at the discretion of the owner and processed in accordance with the criteria applied by the owner.

(e) Prior to the introduction of classified hardware or activation of a classified network connection at an SLT owned or operated facility the following shall have been completed:

(1) Verification and documentation by DHS SLTPS/SMD or the delegated Federal agency of the presence of a GSA Approved security container located within the room/area.

(2) Verification and documentation by DHS SLTPS/SMD or the delegated Federal agency of the presence of an NSA Approved High Security Cross Cut Shredder or other appropriate destruction equipment as cited in Section 4-107 of this directive.

(3) DHS SLTPS/SMD or delegated Federal agency certification/accreditation that the room/area in which the equipment will be deployed meets or exceeds construction and sound attenuation standards for the open storage of classified information as cited in Appendix 3, “State, Local, and Tribal Security Construction Standard for Open Storage Areas.” The “SLT Open Storage Survey Checklist” (Appendix 4) shall be used by DHS SLTPS/SMD or the delegated Federal agency to conduct and record the survey results.

(4) Verification and approval by DHS SLTPS/SMD or the delegated Federal agency of an open storage SOP specific to the location, personnel, and facility and the operational environment of the room/area to be certified.

3-104. Certification/Accreditation for Storage of Classified Information.

a. When a Federal agency has determined that an SLT owned or operated facility has or will have a need to store classified information a "Request for Physical Storage and Associated Secure Capabilities at a State, Local, or Tribal Facility" (Appendix 6) shall be completed by the Federal agency and submitted to DHS SLTPS/SMD.

b. Pursuant to Section 3-101.d.1. of this directive, where an agency enters into an agreement with DHS to retain responsibility for inspection, certification, accreditation, and oversight of SLT owned or operated facilities for which it is the primary sponsor, submission of the "Request for Physical Storage of Classified Information at a State, Local, or Tribal Facility" is not required. In this instance the agency shall perform the functions of DHS SLTPS/SMD indicated below.

c. Within 5 business days of receipt of the request, DHS SLTPS/SMD shall initiate action with the applicable SLT entity to prepare it for certification/accreditation. Preparation shall include:

1. Verification that the applicable SLT entity has appointed an SL and the SL has received appropriate training.

2. Verification that SLT personnel who will access classified information at the applicable SLT facility have been granted the appropriate level security clearance and have received appropriate training.

3. Conduct of a pre-deployment survey by DHS SLTPS/SMD to discuss and communicate necessary security and construction standards with the appointed SL.

4. Establishment of an action plan and subsequent timeline for subsequent certification/accreditation of the SLT facility.

d. When the SLT entity has achieved the necessary security and construction standards, DHS SLTPS/SMD shall conduct a certification/accreditation survey and, if appropriate, issue a certification/accreditation for the storage of classified information applicable to the type of classified media to be deployed.

e. Where such certification/accreditation is issued by an entity other than DHS SLTPS/SMD, a copy of the certification/accreditation shall be provided to DHS SLTPS/SMD pursuant to Section 3-101.d.4. of this directive.

f. Refer to Appendix 7 for a "Security Standards Quick View Matrix" that outlines applicable security standards based on the type of classified activity.

3-105. Oversight and Inspection.

a. On a periodic basis, DHS SLTPS/SMD shall conduct oversight and inspection visits to SLT facilities that have been certified for the storage of classified information. Such visits shall include, but not be limited to, an assessment of the following:

1. The security integrity of the certified facility is maintained in accordance with the initial certification/accreditation documents.

2. Classified information is safeguarded and stored appropriately.

3. The SL and other SLT personnel with access to classified information have received appropriate training.

4. Security standards and the processes for access to classified information are applied in a manner consistent with applicable orders, regulations, and this directive.

b. Oversight and inspection visits shall be announced and coordinated with the sponsoring Federal agency and the applicable SLT SL at least thirty days prior to the date of inspection unless the following apply:

1. An unannounced inspection is warranted based on a report of serious deficiencies or questionable security practices that may jeopardize the integrity of classified information.
2. An announced inspection is warranted but circumstances dictate that the inspection be conducted without benefit of the thirty day notification period.

c. DHS SLTPS/SMD personnel conducting an inspection of a SLT facility shall be afforded full access to all information and facilities necessary to assess compliance with classified information safeguarding and storage standards.

CHAPTER 4

Access, Dissemination, and Safeguarding

4-101. General.

SLTPS entities shall protect all classified information to which they have access or custody and ensure that security standards governing access to and safeguarding of classified information are applied throughout their organizations. This chapter provides security standards to be applied within the SLTPS community for access, dissemination, and safeguarding of classified information.

4-102. Access.

a. Access to classified information shall be limited to persons who have been granted the appropriate level security clearance by a Federal agency and who are performing an official and authorized governmental function in support of a counter-terrorism or homeland security mission whereby the knowledge of the information is necessary in carrying out official duties.

b. When an individual leaves a position or job for which a security clearance and access to classified information were granted, that person must notify DHS SLTPS/SMD or the sponsoring Federal agency to determine if the clearance and access will remain in effect or if a termination briefing should be provided.

4-103. Dissemination.

a. Classified information originating in one agency may be disseminated to another agency or SLTPS entity without the consent of the originating agency, as long as the criteria for access are met, unless the originating agency has determined that prior authorization is required for such dissemination and has marked or indicated such requirement on the medium containing the classified information. When such markings or indicators are present, classified information must not be further disseminated without prior approval of the originating agency. In the case of classified information relating to intelligence sources, methods, and activities, all parties must comply with any directives implemented by the DNI pursuant to E.O. 13526 Sec. 5.1.(c), with respect to the protection of intelligence sources, methods, and activities.

b. Documents created prior to June 28, 2010, shall not be disseminated outside any other agency or SLTPS entity to which it has been made available without the consent of the originating agency. Additionally, documents created on or after June 28, 2010, whose classification is derived from documents created prior to that date, and where the date of the classified source(s) that precede June 28, 2010, is readily apparent, shall not be disseminated outside any other agency or SLTPS entity to which it has been made available without the consent of the originating agency.

c. SLTPS entities shall not disclose classified information to a foreign government or a representative of a foreign government or to any person who is not a U.S. citizen.

d. Classified information shall not be entered into any automated system that has not been specifically certified and accredited for classified processing by a Federal agency.

4-104. Safeguarding.

a. The authorized holder of classified information is personally responsible for the protection and control of the information. Classified information must be safeguarded at all times to prevent loss or compromise and unauthorized disclosure, dissemination, or duplication. Unauthorized disclosure of classified information can be punishable under Federal criminal statutes or, at a minimum, administrative sanctions may be applied, to include revocation of a security clearance. Classified information that is not stored in an approved security container shall be under the constant control of a person having the proper security clearance and need-to-know. The following are additional administrative and operational security standards that shall be followed by SLT personnel for the safeguarding of classified information. These standards also apply to PS personnel when accessing or possessing classified information at an authorized location, e.g., a state fusion center.

1. Use of Classified Cover Sheets. When removed from storage, classified materials shall be kept under constant surveillance, and, when not in immediate use, covered with a standard cover sheet. Cover sheets to be used are: Standard Form (SF) 703-TOP SECRET; SF 704-SECRET; and SF 705-CONFIDENTIAL.

2. End-of-Day Security Checks. Activities that process or store classified information shall establish and implement a system of security checks at the close of each working day to ensure that the area is secure and classified information has been properly stored. The SF 701, "Activity Security Checklist," shall be used to record such checks. A separate end-of-day security check shall be conducted for each room in which classified information is stored and it shall be conducted by an individual who has been granted a security clearance. The following should be included as part of the end-of-day security check:

(a) Check all containers used for the storage of classified material. For mechanical locks, spin the combination dial at least four times, and for digital locks (XO series locks), turn the dial one full turn in each direction. Physically attempt to open each drawer to ensure it is secure.

(b) Check secure telephones to ensure the cards to each unit are not inserted and are not in the immediate vicinity of the unit.

(c) Visually inspect desktops/wastebaskets for the presence of classified materials. Visually inspect copiers, fax machines, and printers to ensure there are no classified materials in, on, or near the devices.

(d) Check other items/devices as deemed necessary for the particular office/work area.

3. Security Container Checks. An integral part of the security check system shall be the securing of open storage areas and security containers used for the storage of classified material. The SF 702, "Security Container Check Sheet," shall be used to record such actions. The SF 702 shall be used to record individual open storage areas and security container openings and closings.

4. Equipment Designations. There shall be no external mark(s) revealing the level of classified information authorized to be, or actually stored in, a given open storage area or security

container or vault, or to the priority assigned to the container for emergency evacuation and destruction. This does not preclude placing a mark or symbol, (e.g., a bar code) on the container for other purposes (e.g., identification and/or inventory purposes).

5. Combinations to Open Storage Areas and Security Containers:

(a) Only persons having an appropriate security clearance and need-to-know shall change combinations to open storage areas and security containers used for the storage of classified information. Where additional guidance is needed as to how to change a combination, contact DHS SLTPS/SMD or the sponsoring Federal agency.

(b) The combination of an open storage area and secure container used for the storage of classified information shall be treated as information having a classification equal to the highest level of the classified information stored therein. The SF Form 700, "Security Container Information," shall be the only manner in which a written record of the combination shall be maintained. When completed and the combination recorded, the SF 700 shall be marked with the appropriate classification level and stored in an approved security container separate from the security container to which the combination applies. Where only one container is available for the storage of classified information, contact DHS SLTPS/SMD or the sponsoring Federal agency for additional guidance on storing the SF 700. Combinations to open storage areas and security containers used for the storage of classified information shall be changed:

(1) When first placed in use;

(2) Whenever an individual knowing the combination no longer requires access to it, unless other sufficient controls exists to prevent access to the lock;

(3) When the combination has been subject to possible compromise;

(4) When taken out of service. Built-in combination locks shall then be reset to the standard combination 50-25-50; combination padlocks shall be reset to the standard combination 10-20-30; and

(5) Every two years.

6. Reproduction of Classified Documents:

(a) Unless restricted by the originating agency, classified information may be reproduced by an SLTPS entity to the extent required by operational needs. When classified information is reproduced, the following standards shall be followed:

(1) Reproduction of classified documents shall be kept to an absolute minimum, consistent with operational requirements.

(2) Any reproduction restrictions cited on the document shall be honored.

(3) Reproduction must only be done on machines that have been approved for classified reproduction by DHS SLTPS/SMD or the sponsoring Federal agency and such machines must not be connected to an unclassified LAN, allow for remote diagnostics, or be equipped with a hard-drive or other devices that retain memory or images.

(4) Any maintenance performed on a machine that has been used for the reproduction of classified information will be done by a cleared person or under the observation of a cleared person. Contact DHS SLTPS/SMD or the sponsoring Federal agency for additional guidance.

(5) Reproduced copies of classified materials are subject to the same safeguards, controls, and accountability procedures as the original.

(6) Waste products generated during reproduction shall be properly protected and disposed of at the same classification level as the information reproduced.

7. Classified Conferences and Workplace Meetings:

(a) Conferences, seminars, symposiums, exhibits, conventions, or other such assemblies consisting of a large and diverse audience, that are to be hosted by an SLTPS entity, and at which classified information may be disclosed, shall only occur when authorized by a Federal agency and only under the security jurisdiction of a Federal agency. If such an assembly is considered, SLTPS entities shall contact DHS SLTPS/SMD or the sponsoring Federal agency for guidance.

(b) Within an SLT facility, conversations that include classified information and other small scale in-house gatherings and impromptu meetings within the workplace, that do not constitute an assembly as cited in 7.(a) above, and at which classified information may be discussed, shall occur only in rooms/areas that have been subjected to a survey by DHS SLTPS/SMD or the sponsoring Federal agency. For example, a private office that has been surveyed and approved for the installation of a secure telephone or a state fusion center that has been certified for open storage of classified information. In these instances, prior authorization from a Federal agency is not required. For such in-house gatherings and other impromptu meetings, it is incumbent upon the SLT host or sponsor of the meeting, in coordination with the servicing SL, to ensure appropriate security measures are in place. The following shall apply:

(1) The meeting shall be held in an area under the security control of a U.S. Government agency, at an appropriately cleared U.S. contractor facility, or at an SLT facility that has been certified for classified activity by DHS SLTPS/SMD or a sponsoring Federal agency.

(2) Ensure that all electronic equipment maintained in the room and capable of transmitting signals wirelessly outside the room, is powered off and disconnected from electrical outlets.

(3) Conduct a sound attenuation test that verifies normal conversational tone from inside the room cannot be heard intelligibly from outside the room – pay particular attention to vents, ducts, and other openings. If public address or other amplification systems are used, conduct the test with these systems on and off.

(4) If appropriate, assign and post cleared host office personnel at exterior doors and hallways to keep the room's perimeter under surveillance and prevent passers-by from stopping and listening.

(5) Verify the identity and security clearance of each participant and ensure security clearances are at least equal to the level of classified information to be disclosed.

(6) Prohibit those without proper authorization and clearance from attending classified portions of the meeting.

(7) Notify each participant and presenter of the highest level of classified information to be presented/discussed and when multiple presentations are given, the specific classification (or unclassified status) of each presentation.

(8) Inform participants of limitations associated with classified portions of the meeting, e.g., prohibitions against photographing, note-taking, audio/video recording, using two-way radios, cellular phones, or other transmitting devices. Audio/video, recording, two-way radios, cell phones and other transmitting devices should be removed from the room prior to the start of classified portions of the brief.

(9) Comply with all security safeguards for classified information.

(10) At the conclusion of the meeting, conduct an inspection of the room to ensure no classified materials have been left behind.

4-105. Storage.

a. Classified information shall be secured under conditions adequate to prevent access by unauthorized persons. The requirements specified in this directive represent acceptable security standards consistent with Federal standards for the storage of classified information.

b. Weapons or items such as funds, jewels, evidence, precious metals or drugs shall not be stored in the same container used to store classified information.

4-106. Standards for Storage Equipment.

a. The General Services Administration (GSA) establishes and publishes minimum standards, specifications, and supply schedules for containers, vault doors, modular vaults, alarm systems, and associated security devices suitable for the storage and protection of classified information.

b. GSA-approved security containers, vault doors, and secure rooms used for the storage of classified information shall have locks that conform to Federal Specification FF-L-2740A when purchasing new equipment. Existing GSA-approved non-FF-L-2740A mechanical combination locks may continue to be used but if repair or replacement is required they shall be replaced with a lock meeting FF-L-2740A standards.

c. Maintenance performed on GSA-approved containers must be in accordance with Federal Standard 809, "Neutralization and Repair of GSA-Approved Containers." When repairs to a GSA-approved container affect its original integrity, the GSA-approved label shall be removed and the container shall no longer be authorized for the storage of classified information.

4-107. Retention and Destruction.

a. Classified information shall be retained only if it is required for effective and efficient operation of the organization, or if law or regulation requires its retention. Documents which are no longer required for operational purposes shall be destroyed in the following manner:

1. National Security Agency (NSA) approved cross-cut shredder listed on the NSA Evaluated Products List (EPL) of High Security Cross-cut shredders. A copy of the EPL can be obtained at the following web site: http://www.nsa.gov/ia/guidance/index.shtml.

2. Burning, wet-pulping, melting, mutilation, chemical decomposition, or pulverizing. In these instances only equipment covered by and listed on an NSA published EPL shall be used.

3. Technical guidance concerning appropriate methods, equipment and standards for the destruction of classified electronic media, processing equipment, components, and the like may be obtained by contacting DHS SLTPS/SMD or the sponsoring Federal agency.

b. Material that has been identified for destruction shall continue to be protected, as appropriate for its classification, until it is actually destroyed.

c. Information classified as Secret or Confidential may be destroyed by one person with an equivalent or higher level security clearance. A destruction certificate is not required unless required by the originator.

4-108. Mailing and Hand-carrying Classified Information.

a. Circumstances in which SLT personnel, and PS personnel that fall under the SLTPS Program, will encounter a need to send classified information by traditional mail, e.g., US Postal Service, are unique and rare. However, should the need arise to send classified information by traditional mail the procedures outlined below shall be followed.

1. Prior to entering classified information into any mailing system the sender shall verify through DHS SLTPS/SMD or the sponsoring Federal agency that:

(a) The intended recipient has the appropriate level security clearance and requires access to the information as required by Section 4-102.a. of this directive.

(b) The intended recipient has the authority and capability to appropriately store the classified information upon receipt.

(c) The intended recipient shall be immediately available to receive and store the classified information when it's anticipated to reach its destination.

2. If an urgent need arises whereby it is essential to the homeland security mission that Secret or Confidential information reach its destination no later than the next day, an overnight delivery service, e.g., FedEx, UPS, etc., may be used. In such cases, the use of an approved commercial overnight delivery service must first be approved by DHS SLTPS/SMD or the sponsoring Federal agency in accordance with 32 C.F.R. Part 2001. When such requests are approved, guidance on use shall be provided to the requestor by DHS SLTPS/SMD or the sponsoring Federal agency.

3. Top Secret information shall NOT be sent through traditional mail under any circumstances. It must be transmitted by cleared courier or approved electronic means. Contact DHS SLTPS/SMD or the sponsoring Federal agency for guidance.

4. Secret or Confidential information may be transmitted by US Postal Service Registered Mail, or US Postal Service Express Mail. When using US Postal Service Express Mail, the following procedures must be adhered to:

(a) Item 11B of the Express Mail transmittal form, "Waiver of Signature Indemnity," must not be completed.

(b) The use of external (street side) express mail collection boxes is prohibited.

(c) A document receipt, DHS Classified Document Record, or similar form approved by a sponsoring Federal agency, shall be prepared by the sender and attached to the document. The purpose of the receipt is to alert the sender that the intended recipient received the materials sent to them.

(d) Upon receipt, the intended recipient shall acknowledge receipt by signing the receipt form and sending it back to the sender. The sender shall retain the signed receipt on file for two years.

(e) If the sender does not receive a signed receipt back from the intended recipient within 20 work days of shipment, the sender shall initiate a tracer to determine the disposition of the sent materials. Contact DHS SLTPS/SMD or the sponsoring Federal agency for assistance.

5. Classified information transmitted or transported outside a facility, whether by traditional mail, overnight delivery, or hand-carried, shall be double wrapped and marked as follows:

(a) The classified information shall first be placed within an "inner" envelope. The inner envelope shall be:

(1) Prominently and conspicuously marked top and bottom on both sides with the highest classification of the materials being transmitted.

(2) Annotated with the complete mailing address, to include the name of the intended recipient, and the complete return address.

(3) Sealed with reinforced tape to prevent inadvertent opening and show evidence of tampering.

(b) The inner envelope shall then be placed within an "outer" envelope. The outer envelope shall be:

(1) Annotated with the complete mailing address and complete return address. DO NOT include personal names on the outer envelope. Instead, in an "Attention" line identify the organization, office code, office symbol, etc., of the intended recipient.

(2) DO NOT place any classification markings on the "outer" envelope. There should be nothing on the outer envelope to reveal the sensitivity of the content or otherwise draw undue attention to it.

(3) Sealed with reinforced tape to prevent inadvertent opening and show evidence of tampering.

6. Classified information shall not be sent through any type of inter-office mail distribution system.

b. When carrying classified information internally within a building but outside of the room in which it is stored, the information shall be covered by the appropriate cover sheet and placed in an unmarked envelope or folder so as not to draw undue attention to the material. The classified information shall remain within the physical possession of the authorized holder until appropriately stored or transferred to another appropriately cleared individual.

c. SLT personnel, and PS personnel that fall under the SLTPS Program, who have a justified need to hand-carry classified information outside of the building where the information is stored are to request approval from DHS SLTPS/SMD or the sponsoring Federal agency. The following procedures apply:

1. Classified information shall not be hand-carried outside of a building unless the person hand-carrying the information has received a classified courier briefing and been issued a classified courier authorization card or one-time authorization letter issued by DHS SLTPS/SMD or the sponsoring Federal agency. The courier card is issued when there is a demonstrated recurring need to transport classified information within the local commuting area. The one-time authorization is issued in instances where a singular need arises to transport classified information within the local commuting area or the need is so infrequent that the issuance of a card is unnecessary.

2. Courier authorization cards or one-time letters shall be issued on a limited basis to individuals to whom DHS or a sponsoring Federal agency has granted a security clearance or whose security clearance has been reciprocally transferred to DHS from another agency.

3. To request a DHS courier authorization card or one-time letter, submit a DHS Form 11000-02, Courier Authorization Request, to DHS SLTPS/SMD. For courier authorization under the sponsorship of another Federal agency, follow the guidance provided by the applicable Federal agency.

4. The courier authorization request must include sufficient justification to support issuance of the card or one-time letter to include why materials must be hand-carried versus the use of other approved means, such as US Postal Service Registered Mail for Secret and Confidential information.

5. Courier authorization cards shall be issued for local metropolitan commuting areas in support of related classified activities. In conjunction with the courier card the bearer, upon request, shall present an official State or Federal government issued photo identification or credential to verify identity.

6. In the rare occurrence that a need arises to transport classified materials aboard a commercial aircraft, prior approval must be obtained from DHS SLTPS/SMD or the sponsoring Federal agency. Contact DHS SLTPS/SMD or the sponsoring Federal agency for guidance.

7. Individuals nominated and approved by DHS SLTPS/SMD or a sponsoring Federal agency as classified couriers shall be provided with specific information on their duties and responsibilities and must sign a briefing acknowledgement form prior to being issued a courier authorization card or one-time letter.

CHAPTER 5

Classification Management

5-101. General.

a. Efficient and economic administration of the classification management program requires the application of effective classification management principles. The integrity of the classification system is dependent upon the knowledge and judgment of officials involved in oversight, implementation, and practical application of the safeguarding and classification process. The consequences of an undefined and inconsistent classification management program are wasted resources, lack of public trust, and potential harm to the national security. Over-classification or unnecessary classification creates an undue economic burden, requires expenditure of funds and commitment of resources, and dilutes the legitimacy of properly classified information, while under-classification or not classifying information when necessary, places the national security at risk. Officials involved in the classification process shall comply with the standards cited in E.O. 13526, its implementing directives, and those cited in this directive and ensure integrity of the system is maintained by implementing a sound classification management program.

b. To the extent practicable and consistent with governing executive orders and regulations, agencies should prepare products for dissemination to the SLTPS community at the lowest sensitivity level possible while still retaining the information's value and relevance to the consumer. Where sanitization to an unclassified or sensitive unclassified level is impractical, unclassified or sensitive unclassified tear lines shall be used to allow for widest dissemination within the SLTPS community, when such dissemination is appropriate.

c. Pursuant to E.O. 13526, agencies shall prepare a classified addendum whenever the classified information constitutes a small portion of an otherwise unclassified document.

d. When making an original classification decision, agencies with original classification authority are encouraged to take into account the intended audience and the impact security classification will have on the ability to share information with officials within the SLTPS community who may have a need for the information in support of counter-terrorism and homeland security efforts. However, classification shall not be avoided for the sole purpose of facilitating information sharing.

e. Notwithstanding an agency's authority to classify information pursuant to E.O. 13526, to the extent practicable, agencies should attempt to avoid classifying information that has been developed by and provided to them by an SLTPS entity and thus limiting reverse dissemination of the same unaltered information from the classifying agency to the SLTPS originators or others within the SLTPS community.

5-102. Derivative Classification.

a. Derivative classification means the incorporating, paraphrasing, restating, or generating in new form information that is already classified (referred to as a classified source), and marking the newly

developed material consistent with the classification markings on an existing source, or, as published in a security classification guide.

b. SLTPS personnel are normally only consumers of classified information and do not have a need to create new products that will contain classified information that has been extracted from an existing classified source. Should there be a need for an SLTPS authorized holder of classified information to perform derivative classification actions the individual must first be approved to derivatively classify by a sponsoring Federal agency. The following shall apply:

1. Before being approved to perform derivative classification actions, SLTPS individuals must be identified, trained, and demonstrate that they are aware of proper derivative classification procedures and markings. Training shall be in accordance with Chapter 6 of this directive.

2. SLT individuals who may have a need to perform derivative classification actions must be identified by local supervisory/management officials to the servicing SL. The SL shall validate the need and submit the name and identifying data, to include security clearance level of the individual, to the sponsoring Federal agency or DHS SLTPS/SMD.

3. PS individuals that fall under this SLTPS Program and who may have a need to perform derivative classification actions must be identified by the sponsoring Federal agency. The sponsoring Federal agency shall validate the need and submit the name and identifying data, to include the security clearance level of the individual, to the office responsible for derivative classification training within the sponsoring Federal agency, or, DHS SLTPS/SMD. PS individuals that fall under this SLTPS Program shall only perform derivative classification actions at a Federal, SLT, or contractor facility that is cleared for classified storage.

4. The sponsoring Federal agency or DHS SLTPS/SMD shall confirm the validity of the request and when appropriate, coordinate the conduct of training.

5. SLTPS individuals who do not receive refresher training at least once every two years shall have their approval to perform derivative classification actions suspended until such time as the required training is received.

6. An individual who is found to be responsible for the commission of a security infraction or violation may be required to take remedial training and/or may have his or her approval to perform derivative classification actions revoked.

7. Any product created by an SLTPS individual that contains classified information is the property of the U.S. Government pursuant to Section 1-105, of this directive, and shall be safeguarded in accordance with this directive and other applicable governing orders, regulations, and directives.

c. If an individual applying derivative classification markings believes the paraphrasing, restating, or summarizing of classified information has changed the level of, or removed the basis for classification, or, believes the markings that appear on a classified source document are unclear or questionable, the individual shall consult the appropriate Federal sponsoring agency or DHS SLTPS/SMD for guidance.

d. When applying derivative classification markings the approved derivative classifier shall:

1. Observe and respect the classification markings cited on the source or in a security classification guide.

2. Carry forward all applicable classification markings, declassification instructions, and handling instructions.

3. Identify him or herself, by name and position or, if applicable, personal identifier, on the "Classified By" line of the newly created document.

4. Markings shall be applied in accordance with the classification marking standards of E.O. 13526 and 32 C.F.R. Part 2001 and classification marking requirements provided by the sponsoring Federal agency or DHS SLTPS/SMD. In addition, classification marking guidance can be obtained through the ISOO published, "Marking Classified National Security Information," which can be obtained at (http://www.archives.gov/isoo/training/marking-booklet.pdf), and the ODNI Controlled Access Program Coordination Office (CAPCO), "Authorized Classification and Control Markings Register and Implementation Manual."

e. Records of Derivative Classification Actions:

1. Persons performing derivative classification actions shall maintain a record of each action taken. For derivatively classified documents, the record shall include the total number of documents derivatively classified, type (e.g., document/e-mail), and classification level.

2. The record shall be maintained by Federal fiscal year (October 1 thru September 30 of each year) and submitted to the applicable Federal agency or DHS SLTPS/SMD as part of annual reporting requirements.

3. Classification actions are counted and reported by document – not by page. For example, a newly created derivatively classified document consisting of multiple pages and containing both SECRET and CONFIDENTIAL information is counted and reported as one derivatively classified document at the SECRET level.

5-103. Classification Challenges.

a. Authorized holders of classified information, who, in good faith, believe its classification status is improper or otherwise questionable, are encouraged and expected to challenge the classification status. Classification challenges fall into one of two categories and shall be processed as described below:

1. Informal Classification Challenges

The classification challenge provision does not prohibit an authorized holder from informally questioning the classification of information through direct and informal contact with the classifier. In fact, informal inquiries are encouraged as a means for holding down the number of formal challenges and for ensuring the integrity of the classification process. When appropriate and when uncertainties exist over the classification status or accuracy of the classification markings, authorized holders of classified information are encouraged to

informally question the classifier to obtain clarification. When a change in classification results from an informal challenge, the challenger shall ensure the official from whom the change was received is authorized to make such a change, and a record of the change, to include the official's name, position, agency, and date is maintained with a file copy of the document. The original classification authority (OCA) making the decision is responsible for notifying all authorized holders of the change in classification or markings.

2. Formal Classification Challenges

(a) Formal challenges to classification shall be in writing and presented to an Original Classification Authority (OCA) having jurisdiction over the challenged information. If the OCA cannot be determined the challenge may be submitted to the CIAO who shall conduct the appropriate research to determine the applicable OCA. Every effort should be made to keep the written correspondence unclassified. However, if the challenge includes classified information it shall be marked and safeguarded accordingly. The written correspondence shall sufficiently describe the information being challenged and can consist of only a question as to why the information is classified or why it is classified at a particular level.

(1) Challenges may come from any authorized holder of the information, to include SLTPS partners.

(2) Individuals submitting a classification challenge shall not be subject to retribution of any kind for bringing such actions. Anonymity can be requested by processing the challenge through the DHS SLTPS/SMD or the CIAO. DHS SLTPS/SMD or the CIAO, as applicable, shall honor a challenger's request for anonymity and serve as the agent for the challenger in processing the challenge.

(3) The OCA receiving the challenge shall provide an initial written response to the challenger within sixty (60) days of receipt.

(4) The agency that has processed the challenge shall provide an opportunity for review by an impartial official or panel.

(5) The individual submitting the challenge has a right to appeal the decision to the Interagency Security Classification Appeals Panel (ISCAP) established by Section 5.3 of E.O. 13526. DHS SLTPS/SMD shall assist with appeals as needed.

(6) Challenged information remains classified and shall be protected at its highest level of classification until a final classification determination is made by an appropriate OCA or as directed by the ISCAP.

CHAPTER 6

Security Training

6-101. General.

Effective security education and training is a cornerstone of the SLTPS Program and essential to the implementation and management of a viable and credible program for the safeguarding of classified information. All SLTPS personnel granted access to classified information are individually responsible for protecting the national security and national interests of the United States. SLTPS managers, supervisors, or equivalents, are responsible for ensuring that personnel are knowledgeable and understand their responsibility to protect information and resources deemed vital to national security.

6-102. Methodology.

Security education, training, and awareness shall be provided to SLTPS personnel on a recurring basis. The DHS SLTPS/SMD shall provide various training methods to be used to administer training, such as briefings, classroom instruction, one-on-one, computer-based, and other distance learning training media. The DHS SLTPS/SMD shall maintain a cadre of trained security personnel to administer, implement, and measure the training's effectiveness and make maximum use of technology, as well as train-the-trainer curriculum, to facilitate a pro-active multi-media campaign of education and training for the SLTPS community.

6-103. Roles and Responsibilities.

a. DHS SLTPS/SMD shall:

1. Develop and distribute standardized security training products that, at a minimum, address the types and coverage of training required by 32 C.F.R. Part 2001.

2. Review existing and proposed security training products developed by other Federal agencies for potential best practices, as well as content and consistency. Leverage best practices and recommend modifications as appropriate.

3. Leverage available technologies and shared resources in the development and distribution of training products. Training methods may include briefings, interactive videos, dissemination of instructional materials, on-line presentations, and other media and methods as deemed appropriate.

4. Maintain a catalog of security training offered for SLTPS personnel and SLTPS personnel participation in them.

5. Maintain a record, by individual, of training completed and training required for SLTPS personnel under the purview of DHS SLTPS/SMD.

6. Ensure compliance with security training requirements are included as part of an inspection and oversight process.

b. Other Federal Agencies shall:

1. Maintain a catalog of security training programs offered for SLTPS personnel by the agency and DHS SLTPS/SMD, and, SLTPS personnel participation in them.

2. To the extent practicable and to promote consistency across the enterprise, leverage available technologies, shared resources, and training products produced by DHS SLTPS/SMD in the conduct of training for SLTPS personnel under their purview. Training methods may include briefings, interactive videos, dissemination of instructional materials, on-line presentations, and other media and methods as deemed appropriate.

3. Where an agency chooses to develop or has developed its own security training products for use in their SLTPS training program, submit the product(s) to DHS SLTPS/SMD.

4. Maintain a record, by individual, of training completed and training required for SLTPS personnel under their purview.

5. Ensure compliance with security training requirements is included as part of the agency's inspection and oversight process.

c. SLTPS entities are responsible for compliance with the security education and training requirements and assessing the efficacy of their efforts on a continuous basis. In addition, they shall:

1. Actively support, promote and monitor security education and training.

2. Ensure records are maintained on a calendar year basis of personnel attending initial, refresher, and specialized security training. At a minimum, these records must reflect the type of training provided, date(s) training was conducted and the name of personnel in attendance.

d. SLTPS Security Liaisons are responsible for:

1. Ensuring security training of SLTPS personnel under their purview is conducted as outlined in this Chapter.

2. Advising the head of the SLTPS entity and DHS SLTPS/SMD or the sponsoring Federal agency, as appropriate, on the status of the organization's security training program.

3. Ensuring training is documented and records are properly maintained.

6-104. Mandatory Training.

a. Initial Security Briefing.

1. Required training for all SLTPS personnel who have met the eligibility standards for access to classified information.

(a) Prior to being granted access to classified information, SLTPS personnel shall receive a comprehensive briefing to inform them of the basic security policies, principles, practices, and criminal, civil, and administrative penalties; as well as the avoidance of over-classification and the processes for challenging the classification of information.

(b) Upon completion of the Initial Security Briefing the individual shall be required to execute a Standard Form 312 (SF-312), "Classified Information Nondisclosure Agreement" and, if applicable, any other approved non-disclosure agreement required by a Federal agency for access to specific types of classified information. Access to classified information is not authorized until a SF 312 or other U.S. Government sanctioned non-disclosure agreement has been executed.

b. Annual Refresher Briefing for Security Clearance Holders.

1. Required training for all SLTPS personnel granted a security clearance.

(a) The Annual Refresher Briefing shall reinforce the policies, principles, and procedures covered during the Initial Security Briefing as well as additional topics as required by 32 C.F.R. Part 2001.

(b) Each SLTPS individual granted a security clearance shall attend or otherwise participate in the Annual Refresher Briefing at least once per calendar year at approximately 12 month intervals.

c. Derivative Classification Training.

1. SLTPS personnel who will or may apply derivative classification markings, regardless of media, shall complete derivative classification training prior to being approved to apply derivative classification markings as stipulated in Section 5.102 of this directive.

(a) Training shall include the proper application of the derivative classification principles, the avoidance of over-classification and, at a minimum, the principles of derivative classification, classification levels, duration of classification, identification and markings, classification prohibitions and limitations, sanctions, classification challenges, security classification guides, and information sharing.

(b) SLTPS personnel must be approved by DHS SLTPS/SMD or a sponsoring Federal agency prior to performing derivative classification functions.

(c) SLTPS personnel who have been approved to perform derivative classification actions shall complete derivative classification refresher training at least once every two years. Individuals who do not complete the training at least once every two years shall have their approval to perform derivative classification actions suspended by DHS SLTPS/SMD or the sponsoring Federal agency, until they have received the proper training.

d. SL Training.

Each SLT individual that has been designated to perform as a SL pursuant to Section 1-110 of this directive shall receive training on the duties and responsibilities of the SL as cited in Appendix 1 of this directive, as well as the policies and procedures for implementation and management of the security requirements prescribed in this directive. The designated SL shall attend any required training within 60 days of his or her designation as the SL.

e. Termination Briefings.

1. SLTPS personnel having access to classified information or security clearance eligibility shall receive a termination briefing (otherwise known as a debriefing) when their access to classified information has been terminated because they have terminated employment, transferred to another SLTPS job where a security clearance is no longer needed, have had their access suspended or revoked, or otherwise no longer require access to classified information.

(a) A termination briefing shall be presented to the individual on the last day of employment, the last day the individual possesses an access authorization, or the day it becomes known that the individual no longer requires access to classified information.

(b) The termination briefing shall be conducted by the SL, DHS SLTPS/SMD, or the sponsoring Federal agency. It shall include coverage as required by 32 C.F.R. Part 2001, and a record acknowledging conduct of the briefing shall become part of the individual's permanent personnel security file.

(c) Should an individual refuse to acknowledge the conduct of a termination briefing the individual shall be debriefed orally and the record shall reflect that the individual refused to execute the termination statement and was orally debriefed.

(d) When a termination briefing is conducted by an SL, a record of the briefing's completion shall be provided by the SL to DHS SLTPS/SMD or the sponsoring Federal agency.

CHAPTER 7

Security Incidents and Sanctions

7-101. General.

a. A security violation or security infraction, collectively called a security incident, is any breach of security regulations, requirements, procedures or guidelines that involves classified information, whether or not a compromise results. No matter how seemingly minor, any individual observing any security infraction or violation must report it immediately, through the SL if applicable, to DHS SLTPS/SMD or the sponsoring Federal agency, so that the incident may be evaluated and any appropriate action taken. Further, DHS SLTPS/SMD or the sponsoring Federal agency, as applicable, shall report security incidents involving the equities of another agency to that agency.

b. Upon receipt of a report of a security violation or infraction, DHS SLTPS/SMD or the sponsoring Federal agency, shall conduct or cause to be conducted, a security inquiry. The purpose of the inquiry shall be to obtain the facts surrounding the cause and effect of the incident, to include whether or not classified information was subjected to compromise.

c. The inquiry official shall document the results of the inquiry in a written report, a copy of which shall be provided, at a minimum, to the senior most management official at the SLT location where the incident occurred, and, where an individual is found to be culpable for a security incident, the individual's personnel security file. For incidents involving PS personnel, a copy of the report shall be provided to the PS individual's immediate supervisor and a copy shall be included in the individual's personnel security file if the individual is determined to be culpable for the incident.

7-102. Reportable Security Incidents. The following are examples of reportable security incidents. This list is a representative sampling and does not address every potential security incident scenario.

a. Leaving a classified file or security container unlocked and unattended either during or after normal working hours.

b. Keeping classified material in a desk or unauthorized cabinet, container, or area.

c. Leaving classified material unsecured or unattended on desks, tables, cabinets, or elsewhere in an unsecured area, either during or after normal working hours.

d. Reproducing, transmitting, or disseminating in any manner classified material without proper authorization.

e. Removing classified material from the work area without proper authorization.

f. Granting anyone, including a visitor, contractor, or employee, access to classified information without verifying both the individual's clearance level and need-to-know.

g. Discussing classified information over the telephone, except in those instances where the discussion of classified information takes place on an approved STE in the secure mode.

h. Discussing classified information in lobbies, cafeterias, corridors, or any other public area where the discussion might be overheard.

i. Carrying safe combinations or classified computer passwords on one's person, writing them on calendar pads, keeping them in desk drawers, or otherwise failing to protect the security of a safe or computer.

j. Failure to mark classified documents properly.

k. Failure to follow appropriate procedures for destruction of classified material.

l. Entering classified information into computers or other electronic systems that are not approved by a Federal agency for the processing of classified information.

m. Introducing non-approved Portable Electronic Devices (PED) or other non-approved wireless devices into an area from which they are prohibited, such as an Open Storage Area.

7-103. Other Reportable Occurrences. The significance of a security incident does not always depend upon whether information was actually compromised. It may also depend on the intentions and attitudes of the individual who committed the incident. The ability and willingness to follow the rules for protection of classified information is a prerequisite for maintaining a security clearance. Although accidental and infrequent minor violations are to be expected, deliberate or repeated failure to follow the rules are not.

a. The following are examples of types of behaviors that are reportable:

1. A pattern of routine security incidents due to inattention, carelessness, or a cynical attitude toward security discipline.

2. Disruptive, violent, or inappropriate behavior within the workplace.

3. Serious financial problems, law enforcement incidents, or other patterns of behavior inconsistent with access to classified information.

7-104. Sanctions.

a. When an individual is found to be responsible for the commission of a security incident, he/she may be subject to administrative, disciplinary, civil, or criminal sanctions, administered by either an agency of the Federal government and/or SLTPS supervisory/management officials, depending on the nature of the incident. The type of sanctions imposed for SLTPS personnel involved in a security incident shall be based on several considerations, including the following:

1. Seriousness of the incident;

2. Intent of the person committing the Security Violation or Infraction;

3. Extent of training the person(s) has received; and

4. Prior history of security violations or infractions.

b. Sanctions that may be imposed upon a SLTPS individual by SLTPS supervisory/management personnel include, but are not limited to, verbal or written counseling, reprimand, suspension without pay, or removal from duty. Additionally, sanctions that may be imposed by the Federal government include suspension or revocation of security clearance, loss or denial of access to classified information, termination of derivative classification authority, or, in the most severe instances, civil or criminal penalties.

c. Sanctions to be imposed shall be determined without consideration of an individual's rank or position.

CHAPTER 8

Contracting for Classified Support

8-101. General.

The awarding of and performance on a contract that includes access to classified national security information by the contractor employees is governed by E.O. 12829, "National Industrial Security Program;" the NISPOM, and Federal Acquisition Regulations. However, these governing policies offer no provisions to allow for elements of SLT entities to directly enter into a contract that, as part of the contract performance, includes access to classified information by the contract employees. Notwithstanding this omission, the Federal government recognizes that in some instances there is a national need for elements of SLT entities to acquire the special skills and expertise that the contract community has to offer in order to further enhance and prosecute the homeland security and counterterrorism mission. As such, SLT entities may have a need to acquire contract support that will include access to classified information. This chapter provides the processes and procedures for the acquisition, award, and oversight of contracts issued directly by SLT entities and that require access to classified national security information.

8-102. Applicability.

The processes and procedures outlined in this chapter are applicable to all SLT entities that have been provided classified access and/or classified capabilities by DHS or another Federal agency and who may have an existing contract, awarded directly by an element of an SLT entity that includes access to classified information by the contract employees, and, those SLT entities that have not yet awarded such a contract but are in the process of or will need to do so in the future. This directive does not apply to classified contract support acquired by a Federal agency in support of an SLT entity.

8-103. Criteria.

a. Only an SLT entity that has a defined counter-terrorism or homeland security mission and is or will be provided access to classified information and/or classified capabilities by DHS or another Federal agency, (e.g., a site where the Homeland Secure Data Network [HSDN] has been deployed – such as a state fusion center), shall be considered for and allowed to contract for classified services or support.

b. Each SLT entity shall have appointed, in writing, an official of the SLT entity to serve as the SL in accordance with Section 1-110 of this directive.

c. Each request by an SLT entity to contract for classified support shall be submitted to DHS SLTPS/SMD or an appropriate office within the sponsoring Federal agency that has management and/or operational responsibility for information sharing and a direct knowledge of the activities of the requesting SLT entity.

d. Requests that are submitted to DHS SLTPS/SMD shall be coordinated through the Office of Intelligence and Analysis, Security Management Branch, for validation. Upon validation, DHS SLTPS/SMD, through the DHS Industrial Security Program Branch, shall process the request.

8-104. Limitations and Restrictions.

a. SLT entities shall not allow a contractor to begin performance on a work effort that includes access to classified information until DHS or the sponsoring Federal agency has entered into an agreement, as cited in this directive, with the applicable contractor that stipulates the conditions under which contractor access to classified information shall occur. SLT entities that may have an existing contract that includes access to classified information and that precedes the date for implementation of this directive shall follow the guidance provided in Section 8-105.(a) of this directive.

b. Only companies that are in possession of a Facility Security Clearance (FCL) issued by an authorized Federal agency under the National Industrial Security Program (NISP) shall be authorized to perform on a contract issued by an SLT entity whereby access to classified information is required. Also, should a contract require storage of classified information by the contractor at a contractor facility, the contractor shall have obtained safeguarding authority by an authorized Federal agency. Refer to Section 8-105.b.2.(b) of this directive for guidance on companies that do not possess an FCL.

c. Only contract employees who are in possession of an active personnel security clearance (PCL) issued by the Defense Security Service (DSS) or another Federal agency, and appropriately certified by the company of employment pursuant to the NISPOM, or the applicable Federal agency, shall be authorized to perform on a contract issued by an SLT entity whereby access to classified information is required.

d. Access to classified information for contracts issued under this directive shall not exceed the SECRET level unless exceptional circumstances exist. Requests for a higher level of classification shall be evaluated on a case-by-case basis by DHS SLTPS/SMD or the sponsoring Federal agency.

e. The contract shall not allow for access to information governed by the Atomic Energy Act of 1954, as amended. This includes, but may not be limited to Restricted Data, Formerly Restricted Data, Unclassified Controlled Nuclear Information, and Safeguards Information.

f. No solicitations shall be issued that will require access to classified information in order for a contract company to prepare a bid on the contract. Therefore, no DD Form 254, "Contract Security Classification Specification," shall be issued during the solicitation phase.

g. A company issued a contract that includes access to classified information pursuant to this directive shall not be authorized to further sub-contract any portion of the contract performance without prior approval by DHS SLTPS/SMD or the sponsoring Federal agency.

8-105. Procedures.

The following procedures are broken down into three sections: procedures for those SLT entities that may have an existing contract, issued prior to publication of this directive, whereby the contract employees currently have access to classified information; procedures for those SLT entities that have not yet awarded such a contract but are in the process of or will need to do so in the future; and follow-on actions.

a. SLT entities with existing contracts that include contractor access to classified information**:**

1. Within 60 days of the date of this directive, the SLT entity shall provide DHS SLTPS/SMD or the sponsoring Federal agency with the following:

(a) A copy of the scope of work

(b) A copy of the contract award documents

(c) The contract award number

(d) The name and full address of each company to which a contract was awarded that includes access to classified information and if classified safeguarding capability at a company facility was required.

2. Upon receipt of the above documents, DHS SLTPS/SMD or the sponsoring Federal agency shall verify with DSS or the Department of Energy (DOE), as appropriate, that the company to which the contract was awarded is in possession of a current and valid FCL and has been issued safeguarding authority, as applicable. Where a company is not in possession of a current and valid FCL all access to classified information by the contract employees shall be immediately terminated and an investigation initiated.

3. Upon verification that the company performing classified work under the contract is in possession of a current and valid FCL, DHS SLTPS/SMD shall validate, per Section 8-103 of this directive, that the SLT entity has been provided access to classified information and/or classified capabilities and there is need for the classified work in support of the homeland security or counterterrorism mission.

4. DHS SLTPS/SMD or the sponsoring Federal agency shall prepare and issue a DD Form 254, "Contract Security Classification Specification." The DD Form 254 shall include specific security instructions applicable to the performance of the contract as it relates to access to classified information and shall be attached to the contractor agreement specified in Section 8-105.a.5. below.

5. DHS SLTPS/SMD or the sponsoring Federal agency shall enter into an agreement with the applicable contractor that will allow for contractor access to classified information in execution of the SLT issued contract and under the terms of the DD Form 254. A sample agreement is provided at Appendix 8.

6. DHS SLTPS/SMD shall facilitate distribution of the agreement and accompanying DD Form 254 to the SLT entity, DSS, and other appropriate agencies as necessary.

7. Thereafter, the contractor shall fall under the security cognizance and oversight of DSS and continues to be subject to the requirements of the NISPOM.

b. SLT entities requesting a new contract that will include access to classified information:

1. Pre-solicitation

(a) At the earliest stage possible the SLT entity shall contact DHS SLTPS/SMD or the sponsoring Federal agency to ensure appropriate coordination and eliminate any potential problems.

(b) The SLT entity shall provide DHS SLTPS/SMD or the sponsoring Federal agency with the following:

(1) A copy of the prospective scope of work, solicitation, request for proposal and/or other applicable contract documents prepared in preparation for a solicitation or request for proposal.

(2) If known, the name and full address of each company that is a prospective bidder/offeror.

(c) Upon receipt of the contract documents, DHS SLTPS/SMD or the sponsoring Federal agency shall validate, per Section 8-103 of this directive, that the SLT entity has been or will be authorized access to classified information and/or classified capabilities and there is a need for the classified work in support of the homeland security or counterterrorism mission.

(d) Based on the verbiage contained in the contract documents, DHS SLTPS/SMD or the sponsoring Federal agency may offer the SLT entity suggested security language for inclusion in the documents.

(e) Where the identity of prospective bidders/offerors is provided, DHS SLTPS/SMD or the sponsoring Federal agency shall verify with DSS or DOE, as appropriate, the existence of a current and valid FCL. The SLT shall then be notified of the existence or non-existence of an FCL for potential bidders/offerors. The lack of an FCL at the pre-solicitation stage should not be used as a determining factor in subsequent contract award.

(f) Further action on the part of DHS SLTPS/SMD or the sponsoring Federal agency shall be held in abeyance pending receipt of bids and/or contract award.

2. Receipt of bids submitted by prospective companies.

(a) Upon receipt of bids by the SLT entity from prospective companies, the SLT entity shall submit the full company name and address of all companies being considered for contract award to DHS SLTPS/SMD or the sponsoring Federal agency.

(b) DHS SLTPS/SMD shall verify with DSS or DOE, as appropriate, the existence of a current and valid FCL for all companies that will be considered for contract award. The lack of a FCL should not be used as a determining factor in contract award. Should the SLT entity select a company for contract award that is not in possession of a current and valid FCL, DHS SLTPS/SMD or the sponsoring Federal agency shall serve as the sponsoring agency in requesting the issuance of an FCL from DSS. Performance on any portion of a contract that requires access to classified information shall not begin until such time as the FCL has been issued by DSS; all appropriate contract employees have

been granted the applicable level of security clearance; a DD Form 254 has been issued; and DHS SLTPS/SMD or the sponsoring Federal agency has entered into an agreement with the prospective contractor as specified in Section 8-105.3.(c) below.

3. Contract award

(a) Upon selection and award of the contract, the SLT entity shall provide DHS SLTPS/SMD or the sponsoring Federal agency with:

(1) A copy of the contract award form(s) indicating the full name and address of the company to which the contract has been awarded, the contract number, the period of performance (including options).

(2) Final copy of the statement of work and/or other similar contract documents.

(b) DHS SLTPS/SMD or the sponsoring Federal agency shall prepare and issue a DD Form 254, "Contract Security Classification Specification." The DD Form 254 shall include specific security instructions applicable to the performance of the contract as it relates to access to classified information and shall be attached to the DHS/contractor agreement specified in Section (4) below.

(c) Upon final approval of a FCL or determination that an appropriate FCL exists, DHS SLTPS/SMD or the sponsoring Federal agency shall enter into an agreement with the applicable contractor that will allow for contractor access to classified information in execution of the SLT issued contract and under the terms of the DD Form 254. Access to classified information by the contractor in the performance of the contract shall not commence until the agreement has been executed and the DD Form 254 issued. A sample agreement is provided at Appendix 8.

(d) Thereafter, the contractor shall fall under the security cognizance and oversight of DSS and continues to be subject to the requirements of the NISPOM.

c. Follow-on Actions.

1. Any modifications to the contract that may have an impact on the contractor's performance as it relates to access to classified information shall be coordinated with DHS SLTPS/SMD or the sponsoring Federal agency prior to the modification being issued. Such modifications include but are not limited to:

(a) Exercise of contract options

(b) Negotiated contract extensions

(c) Modifications affecting a change in work effort

2. The SLT entity shall advise DHS SLTPS/SMD or the sponsoring Federal agency immediately upon termination of a contract regardless of the reason for which the contract was terminated.

Appendix 1

STATE, LOCAL, TRIBAL SECURITY LIAISON

DUTIES AND RESPONSIBILITIES RELATING TO THE SAFEGUARDING OF CLASSIFIED NATIONAL SECURITY INFORMATION

State, Local, Tribal Security Liaison (SL): An official of an SLT entity who has been appointed in writing by the head of the applicable SLT entity, or his/her designee, and who is responsible for implementation, management and oversight of security matters relative to the assigned facility(ies). The official appointed must be in possession of a security clearance issued by DHS or another agency of the Federal government.

The SL shall be primarily responsible for ensuring that Federal classified national security information is handled, safeguarded, and disseminated in accordance with Federal government standards. The SL shall also function as the primary point of contact and liaison with the Department of Homeland Security (DHS) Office of the Chief Security Officer (OSCO), Administrative Security Division, State, Local, Tribal and Private Sector Security Management Division (SLTPS/SMD); the DHS Office of Intelligence and Analysis, Security Management Branch; and in instances where the SLT entity has contracted for support that includes contractor access to classified information, the Defense Security Service (DSS). In cases where a Federal agency has entered into an agreement with DHS pursuant to Section 3-101.c. of this directive, the SL shall function as the primary point of contact with the delegated Federal agency.

SL Duties and Responsibilities:

- Responsible for the management of a security program designed to ensure that Federal classified national security information held and processed within approved facilities is properly safeguarded and protected.

- Ensure that rooms/areas within the applicable facility(ies) where classified information is handled, stored, or discussed meet required Federal security standards and have been appropriately certified by DHS SLTPS/SMD or a sponsoring Federal agency.

- Ensure that SLT officials, Federal officials, contractors and other persons with whom classified information will be discussed or disseminated have been granted the appropriate level security clearance and require access to the information in the performance of their official duties. Access to classified information based solely on rank or position is prohibited and in direct violation of Federal standards for the safeguarding of classified information.

- Maintain a master list of SLT, Federal, and contractor personnel who have been granted a security clearance by the Defense Industrial Security Clearance Office (DISCO) (for contractors), DHS, or another Federal agency, and who are assigned, detailed or attached to the applicable SLT facility(ies). Contractor security clearances shall be provided in writing to the SLT entity by the applicable corporate facility security officer. Where access to a centralized security clearance data base is not available, security clearances of SLT and Federal officials shall be provided in writing to the SLT entity by the security office of the applicable Federal agency that granted the security

clearance. Security clearance certifications (also known as Visit Requests) that are hand-carried by the person to whom the clearance certification applies are not valid and shall not be accepted.

- Ensure security clearances for all personnel performing duties under an approved contract are permanently certified (Perm-Cert) to the DHS Personnel Security Division, or the designated security point of contact for the sponsoring Federal agency, for the duration of the contract and immediately notify stateandlocalclearances@dhs.gov of any changes in employee status (i.e., termination, retirement, resignation, etc.).

- Ensure that contracts anticipated or awarded by the SLT entity that include access to classified information are processed in accordance with Chapter 8 of this directive.

- Manage and provide oversight for contracts awarded by the SLT entity that include access to classified information by the contractors in accordance with Chapter 8 of this directive.

- Monitor the SLT classified contract process to ensure that contractors are not permitted to begin work performance that includes access to classified information until DHS SLTPS/SMD or the sponsoring Federal agency has entered into an agreement with the applicable contractor that stipulates the conditions under which contractor access to classified information is defined.

- Assist in the development and delivery of security training and education to SLT personnel who will be granted a security clearance and access to classified information and ensure a SF 312 is executed for each SLT person under the purview of the SL.

- Ensure compliance with security training requirements of SLT personnel under the purview of the SL and that training records are maintained.

- Ensure that classified national security information is appropriately safeguarded and that approved procedures are followed for the facility's secure operations and classified capabilities.

- Immediately notify the DHS SLTPS/SMD or the sponsoring Federal agency of any infractions or violations involving the handling, storage, safeguarding or dissemination of classified information. Report behavior and/or incidents that are inconsistent with access to classified information. Take immediate steps to appropriately secure classified information that is not properly protected.

Appendix 2

Multi-Use Security Survey Form for State, Local, Tribal and Private Sector Programs

Multi-Use Security Survey Form For State, Local, Tribal and Private Sector Owned or Sponsored Property and Activities			
Section 1. Organization			**Date of Survey**
Name	Organization's Address		
Section 2. Security Liaison Primary Point of Contact			
Name (Print)		Clearance	Clearance Granted By
Phone Number	Fax Number	Secure Phone	Email Address
Section 3. Alternate Point of Contact			
Name (Print)		Clearance	Clearance Granted By
Phone Number	Fax Number	Secure Phone	Email Address
Section 4. Type of Request (*Check all that apply and complete the corresponding checklist below.)*			
a. Collateral Classified Closed Storage Area (Collateral classified information is identified as classified National Security Information under the provisions of E.O. 13526.)			
b. Secure Telecommunications Device: Type (_____)			
c. Secure Fax Machine			
d. Classified Discussion Room/Area			
e. Closed Storage Secure Video Teleconference (SVTC): (*Contact DHS SLTPS SMD to coordinate the Closed Storage SVTC Survey*)			
f. Other Classified Capability (Describe in Remarks Block)			

Section 5. Justification (Requestor must provide)				
Section 6. GSA-Approved Container Information (Required for all requests)				
Container Manufacturer	Container Serial Number	Class of Container		
		5 or 6		
Section 7. Collateral Classified Closed Storage Checklist				
a. Room number/area surveyed:				
b. The GSA-approved security container is located in a private room/office		Yes _	No	N/A
c. The private room/office has a NSA-approved shredder.		Yes	No	N/A
d. The private room/office has a lockable door.		Yes	No	N/A
e. Windows, secondary doors, emergency exits can be secured/locked.		Yes	No	N/A
f. Windows are equipped with blinds or drapes to prevent observation.		Yes	No	N/A
Section 8. Secure Telecommunications Device/Secure Fax Checklist				
a. Room number/area surveyed:				
b. The Secure Telecommunications Device is located in a private room/office.		Yes	No	N/A
c. There is a GSA-approved security container in the room/area.		Yes	No	N/A
d. The private room/office has a NSA-approved shredder.		Yes	No	N/A
e. All classified information, equipment and COMSEC material are stored in a GSA-approved security container when not in use.		Yes	No	N/A
f. The private room/office has a lockable door.		Yes	No	N/A
g. Windows, secondary doors, emergency exits can be secured/locked.___		Yes	No	N/A
h. Windows are equipped with blinds or drapes to prevent observation.		Yes	No	N/A
i. Acoustic Security: Normal conversations held in the private room/office cannot be overheard outside the room. In all adjacent rooms and hallways, outside office speech is unintelligible.		Yes	No	N/A
Section 9. Classified Discussion Room/Area Checklist				

a. Room number/area surveyed:			
b. Federal Agency/Office sponsoring the classified discussion room/area:			
c. The designated room/area has a lockable door or other access control measures to prevent unauthorized access to classified meetings.	Yes	No	N/A
d. Secondary doors, emergency exits can be secured/locked.	Yes	No	N/A
e. All windows which might reasonably afford visual surveillance of personnel, documents, materials, or activities within the facility, are made opaque or equipped with blinds, drapes or other coverings to preclude such visual surveillance.	Yes	No	N/A
f. Acoustic Security: Normal conversations held in the classified discussion room/area cannot be overheard outside the area. In all adjacent rooms and hallways outside the area speech is unintelligible.	Yes	No	N/A
g. If conversations can be heard outside the room, cleared host personnel shall be posted at exterior doors and hallways to keep the room's perimeter under surveillance and to prevent passers-by from stopping and listening.	Yes	No	N/A
h. All electronic equipment maintained in the room capable of transmitting signals outside the room can be powered off and disconnected from electrical outlets.	Yes	No	N/A
i. The sponsored activity has been provided the *SLTPS Program Requirements for Classified Discussions Outside Secure Areas Fact Sheet* .	Yes	No	N/A
Section 10. Remarks			
Section 11. Verifying Official *(Federal Employee)*			
Print Name	Signature	Date	

Title/Grade	Agency	Phone	E-Mail Address

Section 12. Approving Official (*DHS SLTPS SMD Security Officer Use Only*)

Based on the documentation provided and verification by the Federal sponsor in Section 11 above, this facility is approved for closed storage of collateral classified materials and equipment and/or conducting classified discussions at the SECRET level.

Print Name	Signature
Title/Grade	Date

Appendix 3

State, Local, and Tribal (SLT) Security Construction Standard For Open Storage Areas

I. General Policy

A. U.S. Government classified information and systems shall be secured under conditions adequate to prevent access by unauthorized persons. The requirements specified in this State, Local, and Tribal (SLT) Security Construction Standard for Open Storage Areas, represents the minimum standards acceptable for the construction of a secure area that contains U.S. Government SECRET-level classified information systems. This standard is designed to ensure consistency in the application of security standards and the protection and efficient deployment of classified systems, equipment and information.

B. Certification/accreditation of an SLT open storage area constructed in accordance with this directive and issued by DHS SLTPS/SMD, or a delegated Federal Agency that has entered into an security agreement with DHS, shall be reciprocally accepted by all Federal agencies unless the open storage approval was granted with a waiver or exception. In this instance, it is at the discretion of the applicable Federal agency as to whether the open storage certification/accreditation shall be accepted.

C. The DHS SLTPS/SMD shall provide security guidance, inspection, certification, accreditation, and oversight for SLT open storage areas. When a security agreement with another Federal agency is in place the delegated Federal agency shall retain responsibility for inspection, certification, accreditation, and oversight of SLT owned and operated facilities for which it is the primary sponsor.

D. Portable Electronic Devices (PEDs) shall not be introduced into an open storage area. Exceptions shall only be made with written approval from the DHS SLTPS/SMD, or delegated Federal agency in consultation with DHS SLTPS/SMD, the cognizant Information Systems Security Manager and SL. Approvals shall be considered only when the risks associated with the use of such equipment are clearly identified and sufficiently mitigated.

E. Photographic, video, and audio recording are prohibited within the open storage area. DHS SLTPS/SMD, or the delegated Federal agency as applicable, may authorize the use of such equipment for official purposes on a case-by-case basis.

F. Changes affecting the security posture of the open storage area, either physically or operationally, shall be immediately reported by the SL to the DHS SLTPS/SMD or the delegated Federal agency, to include any corrective or mitigating actions taken. If it is determined that the integrity of the open storage area has or will be adversely impacted, certification/accreditation may be suspended or revoked.

II. Waivers

A. SLT requests for waivers to this Standard shall be submitted through the applicable Federal agency sponsor to the DHS SLTPS/SMD. The request shall specify in writing whether it is a request for a waiver or exception, the reason why it is impractical or unreasonable to comply with the

applicable requirement, the duration that a waiver is to remain in force, and appropriate alternative measures to achieve the same result as stipulated in this directive.

B. Federal agency requests for waivers to this standard shall be submitted directly from the agency to the DHS SLTPS/SMD. The request shall specify in writing the reason why it is impractical or unreasonable to comply with the applicable requirement, the duration that a waiver is to remain in force, and appropriate alternative measures to achieve the same result as stipulated in this directive.

III. Certification/Accreditation

A. SLT open storage areas shall be approved based on operational requirements and not for convenience. Where SLT open storage areas are requested to satisfy the installation of one or more classified systems, unless otherwise justified and approved, the secure area authorization shall be limited to the systems and systems connectivity only. All classified documents and removable media shall otherwise require closed storage in an appropriate GSA-approved security container.

B. SLT open storage areas shall have a Standard Operating Procedure (SOP), approved by DHS SLTPS/SMD or the sponsoring Federal agency, that describes operating procedures and established courses of action as a condition for certification/accreditation.

C. When certified and accredited, the DHS SLTPS/SMD or delegated Federal agency as applicable, shall prepare a memorandum citing the specific location, building, room number, level of classified information authorized, restrictions, and any other information deemed appropriate. The DHS SLTPS/SMD shall be the Office of Record for all certifications/accreditations. Delegated Federal agencies shall provide copies of all open storage certifications/accreditations to the DHS SLTPS/SMD.

D. If certification/accreditation is denied, the DHS SLTPS/SMD or the delegated Federal agency as applicable, shall prepare a memorandum citing the reasons for denial and corrective actions necessary to obtain approval.

IV. Open Storage Area Construction Requirements

A. An SLT open storage area shall meet or exceed the construction requirements contained in this standard and have an intrusion detection system (IDS) installed that meets the standards cited herein. These criteria apply to all new construction, reconstruction, alterations, equipment modifications, and repairs of existing areas. This standard shall also be used in evaluating existing areas not previously approved for Secure Video Teleconference (SVTC) operations.

B. The area shall be supported by security-in-depth consisting of a minimum of two additional layers of security. Examples of methods for achieving security-in-depth are:

1. Military installations, embassy compounds, or contractor compounds with a dedicated response force of U.S. persons. A memorandum of understanding or agreement (MOU/MOA) shall be executed outlining response requirements for these facilities.

2. Enclosed vestibule outside of the secure area entrance equipped with an approved high security lock and UL listed alarm equipment installed in accordance with manufacturer's instructions.

3. Separate building access controls/alarms along with elevator controls (e.g., after hours card reader with audit capability) required to gain access to building or elevator.

4. Fenced, alarmed compound with access controlled vehicle gate and/or pedestrian gate.

C. Doors

1. Routine entrance/exit doors shall be kept to an absolute minimum. Where possible, only one single door shall be used for routine entry/exit.

2. Doors shall be constructed of wood, metal, or other solid materials. When doors are used in pairs or a gap exposes the latching mechanism, an astragal (overlapping molding) shall be installed where the doors meet or exposure occurs. Hinges are preferred to be on the secure side of the door. Hinge pins that are exposed to the outer perimeter of the area shall be pinned, brazed, have set screws installed, or be spot-welded to preclude removal. All doors must meet the following criteria:

a. Solid core wood, minimum 1 3/4" thick, or 16 gauge metal cladding over wood or composition material, installed in welded steel frame assembly mounted to 20-gauge or greater metal studs. Knock-down [collapsible jam and header] frame or aluminum frame is not acceptable.

b. Doors and frames shall meet or exceed a Sound Transmission Class (STC) 45 equivalent rating in processing areas. Doors and frames shall meet or exceed an STC 50 equivalent rating in areas where there will be amplified sound. Doors shall have adjustable acoustical gasket around the door with an automatic threshold seal installed in these instances.

c. Doors with windows, louvers, baffle plates, or similar openings are only authorized to be used in areas with no processing or discussion. They shall be secured with 18-gauge expanded metal securely fastened on the inside. If visual access is a factor, the windows shall be covered.

3. Doors shall be equipped with an industrial Grade 1 automatic door closer.

4. For new construction or renovation, entrance doors shall be secured with a GSA-approved, built-in combination lock meeting Federal Specification FF-L-2740-A. The use of a GSA approved, built-in combination lock not meeting Federal Specification FF-L-2740-A is approved for existing locations unless otherwise modified until October 2012, at which time such locks must be replaced with one meeting the proper specification. Other high security locks may be used on a case-by-case basis with the approval of DHS SLTPS/SMD or delegated Federal agency in consultation with DHS SLTPS/SMD. Other doors shall be secured from the inside with a panic bolt (which can be actuated by an alarmed panic bar); a dead bolt; a rigid wood or metal bar (that shall preclude "springing"), which shall extend across the width of the door and be held in position by solid clamps, preferably on the door casing; or by other means approved by DHS

SLTPS/SMD or delegated Federal agency in consultation with DHS SLTPS/SMD, consistent with relevant fire and safety codes.

5. Routine entrance/access doors shall be equipped with a supplemental access control device (e.g., storage room key lock leverset, card reader, cipher lock, etc.,) to control access into the area during working hours. Supplemental access control devices are for access control purposes only and do not provide sufficient security for an unattended open storage area.

6. All door hardware shall meet Grade 1 standards.

7. All key locks shall meet UL 437 standards.

D. Windows. Every effort should be made to construct open storage areas without windows. Windows shall be covered by opaque window film, or by blinds turned to no more than a 45 degree angle, permanently fastened at top and bottom, and not adjustable by the user. The ability to open the window shall be eliminated by either permanently sealing it or installing a locking mechanism on the inside. Windows that open and are less than 18 feet from grade or adjacent roofs, less than 14 feet from other structures, trees, or horizontal openings, or less than 3 feet from openings on the same wall that are not part of the open storage space shall require one of the following:

1. Vertical round iron or steel bars, a minimum of ½" diameter spaced 6" on center. The bars may be mortised into the masonry, built into the frame, or equipped with horizontal crossbars for added strength and support.

2. Vertical flat iron or steel bars, a minimum of 1 ½" x 3/8" spaced 6" on center. The bars may be mortised into the masonry, built into the frame, or equipped with horizontal crossbars for added strength and support.

Note: All fasteners must be welded or specially manufactured to prevent removal.

E. All vents, ducts, and similar openings in excess of 96 square inches (11" diameter for circular ducts) that enter the open storage area must be protected with either bars, or grills, or commercial metal duct sound baffles that meet appropriate sound attenuation class. If one dimension of the duct measures less than six inches, or the duct is less than 96 square inches, bars are not required; however, all ducts must be treated to provide sufficient sound attenuation. If bars are used, they must be 1/2 inch diameter steel welded vertically and horizontally six (6) inches on center; if grills are used, they must be of 18-gauge expanded steel; if commercial sound baffles are used, the baffles or wave forms must be metal permanently installed and no farther apart than six (6) inches in one dimension. A deviation of l/2 inch in vertical and/or horizontal spacing is permissible. An access port to allow visual inspection of the protection in the vent or duct should be installed inside the secure perimeter of the open storage area. If the inspection port must be installed outside the perimeter of the open storage area, it must be locked with a locking device meeting UL 437 standards.

F. Walls.

1. Walls, true floor, and true ceiling shall be permanently constructed and attached to each other. To provide visual evidence of attempted entry, all construction, to include above the false

ceiling and below a raised floor, be done in such a manner as to provide visual evidence of unauthorized penetration. Walls, true floors, and true ceilings shall be uniformly painted to show evidence of unauthorized penetration.

2. Construction shall be of plaster, gypsum wallboard, metal panels, hardboard, wood, plywood, or other materials offering resistance to, and evidence of, unauthorized entry into the area. If insert-type panels are used, a method shall be devised to prevent the removal of such panels without leaving visual evidence of tampering.

3. The perimeter walls of the open storage area shall be true floor to ceiling, or, sufficiently modified to represent a secure enclosure. When wall barriers do not extend to the true ceiling and a false ceiling is created, walls shall be permanently constructed to extend above the false ceiling to the true ceiling using the same building materials as the existing walls.

4. If there is a threat of forced entry (to include high crime areas) as determined by the physical security representative, walls shall be reinforced, slab-to-slab, with 18-gauge expanded metal. The expanded metal shall be spot welded, or fastened by an SLTPS SME approved method every 6 inches to vertical and horizontal metal supports of 20-gauge or greater thickness that has been solidly and permanently attached to the true floor and true ceiling.

V. Associated Equipment Required for Certification/Accreditation

A. SLT open storage area procedures require that classified information not under the personal control and observation of an authorized person shall be stored in a GSA-approved security container equipped with a lock meeting Federal Specification FF-L-2740A. Federal classified system hard-drives that are not designed for routine removal are the only exception to this rule.

B. Open storage areas that maintain a printer connected to a classified system or a secure fax machine must have an NSA approved cross-cut shredder for the destruction of classified information within close proximity to the classified device – within the same room, in an adjacent room, or within an area that precludes the classified from transitioning beyond a controlled environment. Printers shall be dedicated to the classified computer(s) and not routed through a network. The printer shall be physically located within the open storage area. The NSA/CSS Evaluated Products List (EPL) for High Security Crosscut Paper Shredder is available at: http://www.nsa.gov/ia/government/mdg.cfm?MenuID=10.3.1.

VI. Acoustical Security

A. Acoustic controls are designed to protect conversations from being overheard outside the SLT open storage area. Acoustic controls are not intended to prevent a positive audio attack. SLT open storage area perimeter walls, doors, windows, floors, and ceilings, as well as all openings such as vents and ducts, must provide sufficient acoustic control measures to preclude inadvertent disclosure of conversation. This can be achieved through structural enhancements or sound masking if construction or budget restraints prevent structural enhancements from being feasible.

B. The ability of an SLT open storage area to retain sound within the perimeter is rated using a descriptive value, the STC. All SLT open storage areas shall meet the equivalent of Sound Group III –

STC of 45 or better. STC Group IV – STC of 50 or better is required for amplified sound (e.g. secure video teleconferencing, speaker phone).

1. Sound Group III – STC of 45 or better. Loud speech can be faintly heard but not understood. Normal speech is unintelligible.

2. Sound Group IV – STC of 50 or better. Very loud sounds, such as loud singing, brass musical instruments or a radio at full volume can be heard only faintly or not all.

C. In certain cases, there may be a sufficient stand-off distance between a perimeter wall and the operational area, to prevent sound from carrying beyond the perimeter wall. The DHS SLTPS/SMD may waive the STC construction requirement if the STC-45 equivalent rating can be achieved through stand-off distance. The stand-off distance must be subject to inspection, and the area be designated as a no-discussion area. Areas containing amplified sound must be built out to an STC-50 equivalent sound rating.

D. Examples of sound masking include installation of a CD or audio tape player with separate speakers; white noise generators; or other vibrating or noise generating systems that can be installed along the inside perimeter of the area. Where sound traverses through vents, ducts, and other similar openings, install music speakers in or near the opening; or white noise generators in or near the opening. When planning a retrofit, sound masking may be the most cost effective option to meet the acoustic control requirements.

E. Examples of structural enhancements include the use of sound deadening high-density materials in wall construction; use of extra layers of drywall for wall construction; and use of door gaskets for doorframes. Where sound traverses through vents, ducts, and other similar openings, consider installing commercial sound baffles or waveforms. The installation of Z ducts is an effective method of protecting HVAC systems. When planning new construction, structural enhancements should be used to meet the acoustic control requirements.

F. Installation of Equipment and Sound Sources. The sound masking noise generation control source shall be placed within the perimeter of the open storage area and/or in any manner that precludes tampering or evidence thereof. Speakers should be located outside of the area to effectively mask sound and shall be sufficiently protected to prevent manipulation.

G. A functional test to determine appropriate sound attenuation shall be conducted by the inspecting official prior to a room being accredited for open storage of classified. Open storage areas shall be tested for STC in the following manner:

1. With all open storage area doors and windows closed, all perimeter walls and openings, e.g., air ducts – entry and returns, doors, windows, ceiling, etc., shall be tested, along multiple points, to ensure either the Sound Group III or IV is met.

2. Audio test sources shall have a variable sound level output. The output frequency range shall include normal speech audio as well as amplification.

3. Test speakers shall be placed in accordance with manufacturer specifications, and testing shall only be performed by personnel authorized to do so by the DHS SLTPS/SMD.

4. Audio gain of the test source, as directed by the inspecting official, shall produce "loud and/or very loud speech" as defined by Sound Group III and IV levels respectively; or,

5. A "hearability" sound test may be performed by security specialists performing the open storage survey, if electronic testing is not available.

VII. Intrusion Detection System (IDS)

A. The IDS shall be connected to, and monitored by an Underwriters Laboratory (UL) certified central monitoring station. Alarm system installation shall conform to the requirements herein and the standards for IDS approved by the Information Security Oversight Office (ISOO) and using the UL "National Industrial Security System Certificate" with criteria as specified in the UL "National Industrial Security Alarm Description Worksheet." The worksheet is prepared by the UL Certified Alarm Company installing the IDS and the systems operating elements are confirmed by the DHS SLTPS/SMD or delegated Federal agency security office.

B. Evidence of compliance with the requirements of this directive shall consist of a valid UL certificate for the appropriate category of service. This certificate will have been issued to the protected facility by UL, through the alarm installing company. The certificate serves as evidence that the alarm installing company is:

1. Listed as furnishing security systems of the category indicated;

2. Authorized to issue the certificate of installation as representation that the equipment is in compliance with requirements established by UL for the category of service;

3. Subject to the UL Field Counter Check Program, whereby periodic inspections are made of representative alarm installations by UL-certified personnel to verify the correctness of installation practices.

C. IDS requirements:

1. Independent Equipment: When many alarmed areas are protected by one monitoring station, open storage area zones must be clearly distinguishable from the other zones to facilitate a priority response. All sensors shall be installed within the protected area.

2. Premise Control Unit (PCU): No capability should exist to allow changing the access status of the IDS from a location outside the protected area without prior approval of the approval authority. All PCUs (alarm panel) must be located inside the open storage area. Assigned personnel should initiate all changes in access and secure status. Operation of the PCU shall be restricted by use of a keypad and or procedure that verifies authorized use. In the secure mode, any unauthorized entry into the space shall cause an alarm to be transmitted to the monitor station.

3. Backup Power: Emergency backup electrical power shall be provided by battery, generator or both. If batteries are used, then they shall provide a minimum of 24 hours of backup power. An indication shall be sent to the monitoring station when the systems changes to backup power.

4. Keypads: All alarm keypads shall be located inside the open storage area next to the primary entry/exit door.

5. Motion Detection Protection: Motion Detectors shall be a UL 639 listed device. Open storage areas that reasonably afford access to the container or area where classified data is stored shall be protected with motion detection sensors (i.e., ultrasonic, passive infrared, etc.) Use of dual technology is authorized when one technology transmits an alarm condition independently from the other technology. A failed detector shall cause an immediate and continuous alarm condition.

6. Protection of Perimeter Doors: Each perimeter door shall be protected by a UL 634 listed Level 2, High Security Switch (HSS). The HSS removal tamper shall be monitored 24 hours a day regardless if the system is in the access or secure mode of operation.

7. Protection of Emergency Exit-Doors: Each perimeter Emergency Exit-Door shall be protected by a UL 634 listed Level 2, High Security Switch (HSS) and be monitored 24 hours a day regardless if the system is in the access or secure mode of operation.

8. Entrance Door Delay: Entrance door sensors shall have an initial time delay to allow for change in alarm status, but shall not exceed 30 seconds.

9. Windows: All readily accessible windows below 18 feet shall be protected by an appropriate intrusion detection unit installed to signal breakage or penetration of the window or movement of an intruder near the window. Additionally a High Security Switch shall be used on windows that are movable.

10. False and/or Nuisance Alarm: Any alarm signal transmitted in the absence of a detected intrusion, or identified as a nuisance alarm, is a false alarm. A nuisance alarm is the activation of an alarm sensor by some influence for which the sensor was designed but which is not related to an intrusion attempt. All alarms shall be investigated and the results documented. The maintenance program for the IDS should ensure that incidents of false alarms should not exceed one (1) in a period of thirty (30) days per zone.

11. The IDS shall be tested annually to provide assurance that the IDS system is in conformance with this directive. US citizens shall accomplish all IDS testing.

12. IDS PIN codes are For Official Use Only (FOUO) or otherwise sensitive but unclassified, and require additional protection from disclosure. They shall not be transmitted over unsecure phone lines or unencrypted/password protected email. Individual PIN codes shall be assigned to each user. Shared PIN codes are not authorized.

D. The DHS SLTPS/SMD or delegated Federal agency as applicable shall approve contingency protection procedures in the event of an IDS malfunction, power outages, or defective components impairing functional reliability set forth under UL criteria. Contingency procedures shall be described in the SOP. The contingency procedures are approved in conjunction with the certification/accreditation of the open storage area.

E. Contingency measures include:

1. A 24-Amp Hour (equivalent) backup battery or combination of batteries.

2. Emergency generator supplying uninterrupted power to the IDS upon loss of normal power.

3. Implementation of 24-hour continuous protection by personnel maintaining a security clearance on file with the DHS SLTPS/SMD and at the level commensurate with the SLT open storage area until the alarm system malfunction or power outage is corrected.

4. Relocation of all classified materials to another Federally approved open storage area. Coordination with the alternate location should be conducted in advance and the site shall be identified in the SOP.

5. Temporarily terminate classified connectivity.

F. Central Monitoring Station. The central monitoring station may be located at the facility of a UL-listed activity such as:

1. Contractor Monitoring Station, formerly called a proprietary central station (e.g., Honeywell, Tracor, or Johnson Controls);

2. Cleared commercial central station (e.g. ADT, Brinks, or Armor);

3. Protective signal service station (e.g., State Police, County Sheriff's Office, City Police Department or Fire Department having dispatch responsibilities for law enforcement);

4. Alarm monitors shall be in attendance at the alarm monitoring station at all times when the IDS is in operation.

5. The central monitoring station is required to indicate whether or not the system is in working order and to indicate tampering with any element of the systems. Repairs shall be made as soon as possible when the IDS is not fully operational and/or in compliance with UL 2050 standards. Cleared employee(s) shall visually monitor the open storage area on a continuous basis until the alarm system is again fully functional and/or meeting UL 2050 Standards.

6. The IDS shall be activated any time the open storage area is not manned by [authorized] cleared personnel possessing the appropriate security clearance. A record shall be maintained to identify each person activating and deactivating the IDS with the use of Standard Form 702 or through automated means. Such records shall be maintained for one year. These records are sensitive and shall be protected as such, and destroyed by a cross-cut or strip shredder at the end of the one-year period. Every failure of activation or deactivation shall be reviewed by the central monitoring station and upon appropriate determination, be referred to the appropriate security official for investigation when positive confirmation of attempted user is unknown.

7. Records shall be maintained for one year. The record shall indicate time of alarm activation; name(s) of responding personnel; time dispatched to facility area; time responding guard force or law enforcement activity personnel arrived; nature of alarm; and what follow-up actions were accomplished. These records are sensitive and shall be protected as such, and destroyed by a

cross-cut or strip shredder. Continued false alarms shall be reported to the activity having cognizant jurisdiction.

G. Investigative Response to Alarms

1. The following resources may be used when responding to an activated alarm and determining a potential breach: sufficient number of trained security guard personnel, central station guards, municipal, county, or state police, or contracted guard services. Unless, the responding personnel maintain the appropriate security clearance, the responding personnel shall remain outside the open storage area until a responsible party for the area arrives on scene.

2. When the IDS is in an operational mode, designated personnel, cleared to the appropriate level, shall be available at all times to be immediately dispatched to investigate each alarm. On-site emergency response personnel in a full-time functional capacity 24-hours a day and 7 days a week, fulfill this requirement.

3. For a commercial central station, protective monitoring service or residential monitoring station, response personnel dispatched shall have an appropriate security clearance if they have the responsibility and authority to access the area.

4. Guards without a security clearance may be dispatched by a monitoring service or residential monitoring station to the alarm. However, developed response plans shall include notification to a cleared representative of the affected facility for each alarm annunciation. The cleared representative shall be appropriately identified by full name plus a secondary code word, number, or other method. The guards or other response force without security clearances shall remain on the premises and maintain surveillance until a designated, cleared representative of the facility arrives or as instructed by the cleared facility representative.

5. If the alarm activation does not reset or a physical breach of the room is observed, a cleared response team with security clearances must be dispatched. Members of the cleared response team should be identified on a designated list or within a Standard Operating Procedure. The initial response team not maintaining a security clearance (i.e. local law enforcement personnel) must stay on station until relieved by the cleared response team.

6. Contracted guards must be under contract with either the central monitoring station or the facility management entity. However, this does not permit guards to enter the area unless possessing a security clearance in conjunction with a classified contract as associated with a Contract Security Classification Specification, DD-254; as coordinated through DHS SLTPS/SMD.

7. SLT open storage areas require a 30 minute or less alarm response time. Arrangements shall be made with the monitoring station to immediately notify a cleared representative of the facility on receipt of an activated alarm. The representative is required to go immediately to the facility to investigate the alarm and to take appropriate measures to secure the classified material or equipment. The cleared facility representative shall confirm the response time of the investigating guard service, police department, etc.

H. Alarm Installation. Installation of an IDS at a facility, area, or room shall be performed by a UL listed alarm company. When a UL listed alarm company is not available for a specified region, the DHS SLTPS/SMD can waive this requirement under exceptional circumstances on a case-by-case basis. When connected to a commercial central station, Contractor Monitoring Station protective monitoring service, or a residential monitoring station, the service provided shall include line security (i.e., the connecting lines are electronically supervised to detect evidence of tampering or malfunction). If line security is not available, then two independent means of transmitting the alarm signal from the alarmed area to the monitoring station shall be provided. Evidence of line supervision shall be provided to the DHS SLTPS/SMD or the delegated Federal agency security office.

1. Compliance with the requirements set forth in this standard shall meet the respective UL 2050 rating for an intrusion detection system (IDS). NOTE: UL 2050 is a standard that describes the monitoring; signal processing, investigation, servicing, and operation of alarms systems for which a national industrial security systems certificate has been issued by UL in meeting Federal Government criteria. The alarm company certifying the system must also be certified by UL as a listed company for the installation of National Industrial Security Systems. The UL listed alarm company installing the IDS shall provide UL Certification for the required level and an alarm system certificate, which describes the UL rated components, signal process, and alarm monitoring service company, etc. The National Industrial Security System Certificate shall be issued to the protected site by UL, through the alarm certifying company and retained within the approved secure room, area, or facility. All alarm annunciations, responding activities, investigating officials, and reporting of events, and contingencies shall be described within the respective Standard Operating Procedure.

2. Exceptional Cases. If the requirements set forth above cannot be met due to extenuating circumstances, the sponsored organization shall request approval in writing, through the DHS SLTPS/SMD, for an alarm system that is:

a. Monitored by a central control station but responded to by a municipal, county or state law enforcement organization.

b. Connected to alarm receiving equipment located in a municipal, county, or state police station or public emergency services dispatch center. Although the alarm system is activated and deactivated by employees of the sponsored organization, the alarm is monitored and responded to by local law enforcement or a contract security guard force. Police Department alarm response may be requested only when: (1) the facility is located where central control station services are unavailable, and/or (2) a contract security force response cannot be achieved within the required 30 minute time limit.

c. Installation of these type systems must use UL listed equipment and be accomplished by an alarm installation company certified by UL for any of the following categories: National Industrial Security Systems; Proprietary Alarm Systems; Central Station Burglar Alarm Systems; or Police Station Connected Burglar Alarm Systems.

3. When installation of an IDS is proposed that does not meet the requirements set forth in this standard, an installation proposal, explaining how the system will operate, shall be submitted to the DHS SLTPS/SMD or the delegated Federal agency for review. The proposal must include sufficient justification for granting a waiver, if required, and the full name and address of the

police department that will monitor the system and provide the required investigative response upon alarm activation. The name and address of the UL listed/UL certified company that will install the system, inspect, maintain, and repair the equipment shall also be furnished.

4. A 30 minute investigative response time from the police department or other responding force is required, for all SLT open storage areas. A Memorandum of Agreement or letter shall specify that the police department or other monitoring service, immediately notify a cleared representative of the protected site on receipt of an alarm in the open storage area. The representative is required to respond immediately, investigate the alarm, and take appropriate measures to secure the classified material and collect all necessary information regarding the circumstances for reporting as required. This function shall also be addressed within the respective site's Standard Operating Procedure.

5. In exceptional cases where a central station monitoring service is available, but no proprietary security force of the central station or subcontracted guard response is available and where the police department does not agree to respond to alarms and no other manner of investigative response is available, the DHS SLTPS/SMD approval authority may approve cleared employees as the sole means of response. This exceptional function shall be annotated within the respective site's Standard Operating Procedure.

Appendix 4

State, Local, and Tribal (SLT) Open Storage Survey Checklist

This checklist documents and verifies that classified information and systems shall be secured under conditions adequate to detect and deter access by unauthorized persons. This checklist represents the minimum standards acceptable for the construction of an SLT Open Storage Area. References cited for each checklist item are from the Classified National Security information Program for SLTPS Entities Implementing Directive.

To use this document:

- Check "Yes" if the checklist item for the surveyed area applies or currently exists. Use the Remarks section for additional comments.
- Check "No" if the checklist item applies but does not exist as required. *All "No" answers must be explained in the Remarks section.*

- Check "N/A" if the checklist item isn't applicable.

Section 1. Organization Data	**Date of Survey**
a. Organization: _____ _____	**b. Organization's Mailing Address** (*Include Floor and Room Number*): _____ _____ ___
c. Point Of Contact (POC) Name/Phone/Email Address: _____ _____	
Section 2. Type of Facility:	
☐ Fusion Center ☐ Emergency Management ☐ State Government ☐State Police ☐Local Government ☐Local Police ☐Other (*Describe*):	

Section 3. Administrative Security Requirements	**YES**	**NO**	**N/A**
a. Only information up to the SECRET level is processed, discussed or stored in the area. **(Ref: Chapter 3, Section 3-101.c.)**			
b. A Standard Operating Procedure (SOP) detailing day-to-day operations of the area has been reviewed and approved by a Federal agency.. **(Ref: Appendix 3, Section III.B.)**			

c. All classified information, removable media, and equipment are/will be stored in GSA approved security containers. A classified system hard-drive that is not designed for routine removal is the only exception to this requirement. **(Ref: Appendix 3, Section III.A.)**			
d. There is a dedicated response capable of responding to unannounced alarms within 30 minutes of alarm annunciation. (**Insert name of response force:** **(**_____) **(Ref: Appendix 3, Section VII.G.7.)**			
e. Cleared facility representatives are available to respond and assist the guard force. (**Ref: Appendix 3, Section VII.G.4.)**			
f. The area contains a NSA approved shredder and GSA approved security container. **(Ref: Appendix 3, Section V.A. and V. B.**)			
g. Portable electronic devices as well as photographic, video, and audio recording units are prohibited from the open storage area. **(Ref: Appendix 3, Section I.D, and I.E.)**			
Section 4. Secure Area Construction Requirements			
a. The area is supported by security-in-depth consisting of a minimum of two additional layers of security. **(Ref: Appendix 3, Section IV.B.)**			
b. Doors are equipped with heavy-duty builder's hardware (Grade 1 Standard). **(Ref: Appendix 3, Section IV.C.6.)**			
c. All ducts, pipes, registers, sewers and tunnels in excess of 96 square inches in area and over 6 inches in its smallest dimension is secured by 18-gauge expanded metal or wire mesh or by ½ " rigid metal bars, steel welded vertically and horizontally 6 inches on center. **(Ref: Appendix 3, Section IV.E.)**			
d. Commercial sound baffles or wave forms are used in vent ducts and are metal, permanently installed, and are no further apart than six inches. **(Ref: Appendix 3, Section IV.E.)**			
e. (1) Inspection ports on ducts are located on the inside of the open storage area, and are capable of providing visual evidence of the expanded metal or man-bars on the wall inside the duct. (2) Inspection ports located outside the open storage area have locking devices that meet UL 437 standards. **(Ref: Appendix 3, Section IV.E.)**			
f. Ducts/vents are configured with a sound attenuation device or sound masking is used. **(Ref: Appendix 3, Section VI.E.)**			

g. Entrance door is secured with a built-in GSA approved combination lock that meets Federal Specification FF-L-2740-A. **(Ref: Appendix 3, Section IV.C.4.)**			
Section 5. Doors			
a. Only one single door is used as for routine entrance and exit. **(Ref: Appendix 3, Section IV.C.1.)**			
b. The entrance door is equipped with a built-in GSA-approved combination lock meeting Federal Specification FF-L-2740-A. **(Ref: Appendix 3, Section IV.C.4.)**			
c. The entrance door is equipped with an automatic door closer, acoustical gaskets, and automatic door bottom sweep. **(Ref: Appendix 3, Section IV.C.2.b. and C.3.)**			
d. The entrance door is equipped with a supplemental access control device (e.g., card reader, cipher lock, etc.,) to control access into the area during working hours. **(Ref: Appendix 3, Section IV.C.5.)**			
e. Doors equipped with unsecure hinge pins located on the exterior side of the door into an uncontrolled area outside the open storage area have hinge pins peened, brazed, spot welded or have set screws installed to prevent removal of the door. **(Ref: Appendix 3, Section IV.C.2)**			
f. (1) All doors and frames are constructed of wood, metal, or other solid materials and meet STC 45 or 50. (2) Solid wood core door, a minimum of 1 3/4 inches thick or 16 gauge metal cladding over wood or composition materials, a minimum of 1 3/4 inches thick. The metal cladding is continuous and covers the entire front surface of the door. **(Ref: Appendix 3, Section IV.C.2. a. and b.)**			
g. Emergency exit doors are constructed of material equivalent in strength and density to the entrance door. Emergency exit doors are secured from the inside with a panic bolt which can be actuated by an alarmed panic bar; a dead bolt; a rigid wood or metal bar, which extends across the width of the door. It is held in position by solid clamps, preferably on the door casing; or by other means approved by the primary approval authority and consistent with relevant fire and safety codes. **(Ref: Appendix 3, Section IV.C.4.)**			
h. Key locks meet UL 437 standards and are maintained under positive control. **(Ref: Appendix 3, Section IV.C.7.)**			
Section 6. Windows			
a. All perimeter windows are inoperable. (Windows can be made inoperable by either permanently sealing them or equipping them on the inside with a locking mechanism.) **(Ref: Appendix 3, Section IV.D.)**			

b. All windows which might reasonably afford visual surveillance of classified material, activities, or systems within the facility, are made opaque or equipped with blinds, drapes or other coverings to preclude observation from outside. **(Ref: Appendix 3, Section IV.D.)**			
c. Windows that are less than 18 feet from the ground or other platform, less than 14 feet from other structures, trees, etc, or less than 3 feet from openings on the same wall that are not part of the open storage area are protected from forced entry by ½" metal bars (separated by no more than 6 inches), plus crossbars to prevent spreading. **(Ref: Appendix 3, Section IV.D, 1, and 2)**			

Section 7. Walls

a. The open storage area walls, ceiling, and floor are constructed of permanent materials (e.g. plaster, gypsum, wallboard, wood/plywood, 18-gauge wire mesh/expanded metal or other materials) offering resistance to and evidence of unauthorized entry. They are permanently constructed and attached to each other. **(Ref: Appendix 3, Section IV.F.)**			
b. If insert-type panels are used, a method has been devised to prevent the removal of the panels without leaving visual evidence of tampering. **(Ref: Appendix 3, Section IV.F.2.)**			
c. At a minimum, the perimeter walls of the Secure Area must be true floor to true ceiling or sufficiently modified to represent a secure enclosure. **(Ref: Appendix 3, Section IV.F.3.)**			

d. **Perimeter Walls Structure: Check** all that apply and expand as necessary. **Drawing of space must be included**

	Interior Wall	Exterior Wall	Brick	Drywall	Concrete	Wood	Expanded Metal	Glass	Other	True floor to true ceiling (Y or N)
Wall #1										
Wall #2										
Wall #3										
Wall #4										

e. The space is constructed to meet or exceed a Sound Transmission Class (STC) of 45. (*Note: STC 45 is the minimum standard for an open storage area*) **(Ref: Appendix 3, Section VI.B.)**			
f. Sound attenuation requirements are met with structural enhancements such as sound deadening high-density materials in wall construction and/or other sound attenuation devices. **(Ref: Appendix 3, Section VI.A. and E.)**			
g. If a secure video teleconferencing system will be installed in the room the area conforms to STC 50 requirements. **(Ref: Appendix 3, Section VI.B.)**			
h. Sound masking of the room provides adequate protection to preclude intelligible sounds from traversing through the walls. **(Ref: Appendix 3, Section VI.D. and E.)**			
i. When wall barriers do not extend to the true ceiling and a false ceiling is created, walls are permanently constructed to extend above the false ceiling to the true ceiling using similar building materials as the existing walls or 18 gauge expanded metal mesh or the false ceiling is reinforced with 18 gauge expanded metal to serve as the true ceiling. **(Ref: Appendix 3, Section IV.F.3 and IV.F.4**			
Section 8. Intrusion Detection System (IDS)			
a. An intrusion detection system (IDS) is installed. The IDS conforms to standards approved by the Information Security Oversight Office. The IDS meets Underwriters Laboratory (UL) Standard 2050 and was installed by a UL listed alarm company. A valid "National Industrial Security System Certificate" is available for review. **(Ref: Appendix 3, Section VII.A.)**			
b. The IDS is connected to and monitored by a UL certified central monitoring station. **(Ref: Appendix 3, Section VII.A.)**			
c. The Central Monitoring Station is located at the facility of an UL listed: **(***Circle one***)** (1) Contractor Monitoring Station (2) Cleared Commercial Central Station (3) Cleared Protective Signal Service Station (4) Cleared Residential Monitoring Station **(Ref: Appendix 3, Section VII.F.)**			
d. The service provided by the Central Monitoring Station includes line security to detect evidence of tampering and malfunction. **(Ref: Appendix 3, Section VII.F.5. and VII.H)**			
e. All perimeter doors are protected by a High Security Switch (HSS) that meets the standards of UL 634 – Level 2. **(Ref: Appendix 3, Section VII.C.6.)**			
f. Areas within the secure area that reasonably afford access to the container or space where classified data is stored are protected with motion detection sensors inside the area. Motion detectors are a UL 639 listed device. **Ref: Appendix 3, Section VII.C.5.)**			

g. All alarm sensors, the Perimeter Control Unit (PCU), and the alarm signal lines are tamper proof. **(Ref: Appendix 3, Section VII.F.5. and VII.H.)**			
h. The PCU and alarm keypad is located within the open storage area. **(Ref: Appendix 3, Section VII.C.2. and 4.)**			
i. Emergency power is available for the IDS (*Identify)*. (1) Battery (2) Generator (3) Other (*Describe*) **(Ref: Appendix 3, Section VII. C. 3.)**			
j. If batteries are used for emergency backup power, they provide a minimum of 24 amp hours of backup power and are maintained at full charge by automatic charging circuits. **(Ref: Appendix 3, Section VII.E.1. and VII.C.3)**			
k. The IDS is tested and documented at least once every year. **(Ref: Appendix 3, Section VII.C.11.)**			
Section 9. Acoustical Protection			
a. All open storage area perimeter walls meet Sound Group III, STC of 45 or better. **(Ref: Appendix 3, Section VI.B)**			
b. If SVTC system is deployed in the open storage area, the area meets the acoustical security requirements of Sound Group IV - STC of 50 or better. **(Ref: Appendix 3, Section VI.B. and C.)**			
c. If enhanced construction and baffling measures have been determined to be inadequate for meeting Sound Group III or IV, as appropriate, sound masking has been employed. **(Ref: Appendix 3, Section VI. A. and D.)**			
d. A sufficient stand-off distance between a perimeter wall and the operational area to prevent sound from carrying beyond the perimeter wall is used to mitigate acoustical deficiencies that do not meet STC 45. **(Ref: Appendix 3, Section VI. C.)**			
e. *Blank – for future use*			
f. The sound masking noise generation control unit is located within the perimeter of the open storage area and precludes tampering with any portion of the system. **(Ref: Appendix 3, Section VI. F.)**			
g. Speakers/transducers are placed outside the room, close to doors, windows, common perimeter walls, vents/ducts, and any other means by which intelligible sound can leave the area. **(Ref: Appendix 3, Section VI. F.)**			

h. The speakers or transducers are optimally placed and the system volume has been set and fixed. The level for each speaker was determined by listening to conversations occurring within the open storage area and the masking sound and adjusting the volume level until conversations are not intelligible from outside the open storage area. **(Ref: Appendix 3, Section VI.G.4)**			
i. A functional test is conducted to determine appropriate sound attenuation by the inspecting official prior to certification for open storage of classified. With all open storage area doors and windows closed, all perimeter walls and openings (air ducts – entry and return, doors, windows, ceiling, etc.) shall be tested along multiple points. **(Ref: Appendix 3, Section VI. G. and G.1)**			
Remarks:			

Inspecting Official Name *(Print)* *Signature* *Date*

Appendix 5

SLT Closed Storage Secure Video Teleconferencing Processing Area Survey

This checklist contains the minimum standards acceptable for the discussion, processing, storage of classified information and the operation of specific Secret-level classified systems and/or a Secure Video Teleconferencing systems in a designated closed storage area[4]. It documents and verifies that Federal classified information and systems shall be secured under conditions adequate to prevent access by unauthorized persons.

To use this document:

- Check "Yes" if the checklist item for the surveyed area applies or currently exists.
- Check "No" if the checklist item applies but does not exist as required. **All "No" answers must be explained in the remarks section.**
- Check "N/A" if the checklist item does not apply, and explain in the remarks section.

Closed Storage Secure Video Teleconferencing Processing Area Survey
Section 1. Organization Data
a. Organization:
b. Organization's Mailing Address (include floor and room number):
c. Point Of Contact (POC) Name:
d. POC Phone/Email Address:
Section 2. Security Survey Data
a. DHS SLTPS SMD or delegated Federal Agency Security Office:
b. Survey Conducted by: (Name, Position/Title and Phone number)
c. Date of Survey:
d. Highest Level of Classified Processing: SECRET

[4] . A Closed Storage Processing Area is established when an organization has been sponsored for and has a requirement to process classified information using an approved Closed Storage configuration.

Section 3. Type of Facility			
☐Federal Government ☐State and Local Fusion Center ☐ State Government ☐Other (Describe)			
Section 4. Closed Storage Security Requirements			
a. Only SECRET information and equipment is processed, discussed or stored in the area.	**YES**	**NO**	**N/A**
b. An approved Standard Operating Procedures (SOP) for the area is available for review.	**YES**	**NO**	**N/A**
c. The room/facility is equipped with a GSA approved Class 5 or Class 6 security container for the storage of classified documents, diskettes, CDs/DVDs, COMSEC Keying Materials, and equipment.	**YES**	**NO**	**N/A**
d. The room/facility is equipped with an NSA Approved Shedder for the destruction of classified material.	**YES**	**NO**	**N/A**
e. A secure video teleconferencing system (SVTC) is to be installed in the area. (If **YES**, the acoustical requirements described in Section 7. must be met and any mitigating factors employed prior to installation.)	**YES**	**NO**	**N/A**
f. All gaps/holes around or near the air vent/pipe penetrations to the closed storage area perimeter are sealed.	**YES**	**NO**	**N/A**
g. Only one single door is used as the primary entrance/exit door.	**YES**	**NO**	**N/A**
h. The primary entrance door is equipped with a lock. (Circle all that apply) Key lock Cipher lock Card Reader	**YES**	**NO**	**N/A**
i. Closed storage area entrance and emergency exit doors are consistent with room perimeter wall construction. Doors are: Solid wood core door, a minimum of 1 3/4 inches thick or sixteen gauge metal cladding over wood or composition materials, a minimum of 1 ¾ inches thick or are rated at STC-45 or STC-50 as applicable.	**YES**	**NO**	**N/A**
j. Emergency exit door(s) is constructed of material equivalent in strength and density to the main entrance door. The emergency exit door is configured to prevent unauthorized entry.	**YES**	**NO**	**N/A**

Section 5. Windows			
a. All perimeter windows can be locked.	**YES**	**NO**	**N/A**
b. All windows which might reasonably afford visual surveillance of personnel, documents, materials, or activities within the facility, are made opaque or equipped with blinds, drapes or other coverings to preclude observation from outside.	**YES**	**NO**	**N/A**
Section 6. Walls			
a. The closed storage area walls, ceiling, and floor are constructed of permanent materials (e.g. plaster, gypsum, wallboard, wood/plywood, or other materials).	**YES**	**NO**	**N/A**
b. Room construction must be sufficient to meet the acoustical security requirements for Sound Group III - STC of 45 or better: Loud speech can be faintly heard but not understood. Normal speech is unintelligible.)	**YES**	**NO**	**N/A**
Section 7. Secure Video Teleconferencing (SVTC) Requirements			
a. An SVTC system is to be deployed in the closed storage area. (If YES, the area must meet the acoustical security requirements for Sound Group IV - STC of 50 or better: Very loud sounds, such as loud singing, brass musical instruments or a radio at full volume can be heard only faintly or not at all.)	**YES**	**NO**	**N/A**
b. The SVTC systems deployed in the closed storage processing is configured for the required use of earphones. (If YES, the area must meet the acoustical security requirements for Sound Group III - STC of 45 or better: Loud speech can be faintly heard but not understood. Normal speech is unintelligible.)	**YES**	**NO**	**N/A**
Section 8. Intrusion Detection System (IDS) (Not Required) (**NOTE**: Complete this section only if an intrusion detection alarm system (IDS) is installed.)			
a. The IDS conforms to standards set forth by Underwriters Laboratory (UL) Standard 2050 and was installed by a UL listed alarm company. A valid UL Certificate is available for review.	**YES**	**NO**	**N/A**
b. The IDS is connected to and monitored by a central monitoring station.	**YES**	**NO**	**N/A**

c. The Central Monitoring Station is located at the facility of an UL listed: **(Circle one.)** (1) Contractor Monitoring Station (2) Cleared Commercial Central Station (3) Cleared Protective Signal Service Station (4) Cleared Residential Monitoring Station	**YES**	**NO**	**N/A**
d. The service provided by the Central Monitoring Station includes line security to detect evidence of tampering and malfunction.	**YES**	**NO**	**N/A**
e. All perimeter doors are protected by a balanced magnetic switch (BMS) that meets the standards of UL-634 Level 2 (High Security)	**YES**	**NO**	**N/A**
f. Areas within the closed storage area that reasonably afford access to the container or space where classified data is stored are protected with motion detection sensors inside the closed storage area.	**YES**	**NO**	**N/A**
g. All alarm sensors, the Premise Control Unit (PCU), and the alarm signal line are tamper protected.	**YES**	**NO**	**N/A**
h. The PCU is located within the closed storage area. (PCU must be located within the closed storage area.)	**YES**	**NO**	**N/A**
i. Emergency power is available for the IDS (Circle one). (1) Battery (2) Generator (3) Other (Describe)	**YES**	**NO**	**N/A**
k. The IDS is manually tested and documented every six months.	**YES**	**NO**	**N/A**
Remarks			

Appendix 6

Request for Physical Storage and Associated Secure Capabilities at an SLT Facility

Request for Physical Storage and Associated Secure Capabilities at an SLT Facility	
This form is completed by the designated Federal Sponsoring Official to endorse physical storage and associated secure capabilities for a State, Local, Tribal or Private Sector entity. When completed submit this form to the DHS SLTPS/SMD.	
Section 1: Federal Sponsor Endorsing Access	
Designated Federal Sponsoring Official/Agency/Sponsoring Official Name/Title/Activity/Contact Information	*Specific Date Capability Required*
Federal Agency Security POC (Name/Phone/Email)	
Section 2: Sponsored SLT Organization *(Note: Sponsored organization must have the security environment verified and certified prior to the issuance of equipment or other capability.)*	
Organization/Activity Name	
Mailing Address (Include Room No and Zip Code)	

Section 3: Sponsored Organization Point of Contacts (POC)	
Security Liaison (Name/Phone/Email)	
Section 4: Requested Capability (Check all items being requested.)	
a. Closed Storage for Collateral Classified Information	
b. Certified Open Storage for HSDN	
c. Information Processing System (IPS) Container	
d. Classified Network Printer	
e. Secure Communications Equipment (i.e. STE, OMNI, etc.)	
f. Secure Video Teleconferencing (SVTC)	
g. Secure Fax Machine	
h. Courier Card (s)	
i. Other (Specify)	
Section 5: DHS SLTPS SMD Use Only	
Receiving Official (Name & Title)	*Date Received*
Assignment/Comments/Remarks	

Appendix 7

Security Standards Quick View Matrix

SECURITY STANDARDS QUICK-VIEW	[1]Federal Personnel Security Clearance	ISDN Telephone Line	GSA Approved Storage Container	[2]Private Office	[3]Document Shredder	[4]Intrusion Detection Alarm System	[5]Federal Agency Approved Open Storage Area	[6]Standard Operating Procedures
Person to Person verbal-only access to classified information	**X**							
Secure Telephone (STE)	**X**	**X** For STE Only	**X**	**X**	Recommended[7]			
Secure Telephone (STE) w/Secure Fax	**X**	**X** For STE Only	**X**	**X**	**X**			
Secure Video Teleconference	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
Closed Storage of Confidential and/or Secret Information	**X**		**X**	**X**	**X**			
Installation of Classified Computer System, e.g., HSDN	**X**		**X**	**X**	**X**	**X**	**X**	**X**

[1] Security Clearance must be granted by a Federal Executive Branch agency and be equal to or higher than the level of classified information the person will access.
[2] STE shall be installed in a private office or area having sufficient acoustical protection and physical controls to prevent conversation being overheard by unauthorized persons.
[3] For the destruction of classified information, document shredders must meet Federal standards for particle size. Contact the DHS SLTPS/SMD for approved shredders and vendors.
[4] Refer to guidance on open storage areas for information on Intrusion Detection Alarm Systems.
[5] Refer to guidance on open storage areas for information on structural requirements.
[6] Refer to guidance on open storage areas for information on Standard Operating Procedures.
[7] If the potential exists that handwritten notes will be taken based on classified conversations conducted over a secure phone then an approved shredder must be available.

Appendix 8

Sponsoring Federal Agency Agreement with State Contractor

MEMORANDUM OF AGREEMENT
BETWEEN THE SPONSORING FEDERAL AGENCY DESIGNATED OFFICE
AND
(IDENTIFICATION OF CONTRACTING COMPANY)
REGARDING ACCESS TO CLASSIFIED NATIONAL SECURITY INFORMATION
IN SUPPORT OF A CONTRACT ISSUED BY
(IDENTIFICATION OF STATE ENTITY)

1. PARTIES: The parties to this Memorandum of Agreement (MOA) are the Sponsoring Federal Agency Designated Office and IDENTIFICATION OF CONTRACTING COMPANY TO INCLUDE NAME, ADDRESS, AND CAGE CODE.

2. AUTHORITY: This MOA is authorized under the provisions of:

a. Executive Order 13549, Classified National Security information Program for State, Local, Tribal and Private Sector entities

b. Executive Order 13526, Classified National Security Information

c. Executive Order 12968, Access to Classified National Security Information

d. Executive Order 12829, as amended, National Industrial Security Program

e. Applicable Sponsoring Federal Agency Policy

3. PURPOSE: Executive Order (E.O.) 12829 does not allow for agencies of State or Local government entities to directly enter into contracts that, as part of the contract performance, includes access to classified information (as defined in Executive Order 13526, "Classified National Security Information") by the contract employees. Further, E.O. 12829 does not allow for the direct receipt or dissemination of classified information between a State or Local entity and the contractor. Specifically, section 101.(a) of E.O. 12829 states in part: "The purpose of this program is to safeguard classified information that may be released or has been released to current, prospective, or former contractors, licensees, or grantees of *United States agencies*…The National Industrial Security Program shall be applicable to all *executive branch* departments and agencies."

As such, E.O. 13549 integrated the SLT community into the National Industrial Security Program by allowing for the capability of SLT to entities to contract for classified support. E.O. 13549 states: "The National Industrial Security program established in Executive Order 12829, as amended, shall govern the access to and safeguarding of classified information that is released to contractors, licensees, and grantees of SLT entities."

The purpose of this MOA is to ensure oversight of the protection of classified information, as required under E.O. 12829, and to establish a relationship between DHS and IDENTIFICATION OF CONTRACTING COMPANY in order for IDENTIFICATION OF CONTRACTING COMPANY to receive and disseminate classified information in support of a contract awarded by a State or Local entity. This MOA and accompanying DD Form 254, "Contract Security Classification Specification," set forth the terms and conditions by which cleared employees of IDENTIFICATION OF CONTRACTING COMPANY shall be required to receive and disseminate classified information in the performance of CONTRACT NUMBER issued by IDENTIFICATION OF STATE ENTITY. Pursuant to this agreement and E.O. 12829, the Defense Security Service shall have security cognizance under the National Industrial Security Program.

4. RESPONSIBILITIES:

a. Sponsoring Federal Agency Designated Office

(1) Provide the applicable contractor with specific security standards, receipt and dissemination restrictions, and classification guidance through issuance of a DD Form 254, which shall be a mandatory addendum to this MOA.

(2) Serve as the approval authority for the receipt and dissemination of classified information between the applicable contractor and State and Local entity.

b. Contractor

(1) Comply with the specific security standards, receipt and dissemination restrictions, and classification guidance as cited in the DD Form 254 that is an addendum to this MOA.

(2) Comply with the requirements of E.O. 12829 and the National Industrial Security Program Operating Manual (NISPOM) for requirements not covered by the DD Form 254 that is an addendum to this MOA.

5. POINTS OF CONTACT:

Sponsoring Federal Agency Designated Office

POC:

Title/Office:

Organization:

Address:

Office Phone:

Fax:

Email:

CONTRACTOR

POC:

Title/Office:

Organization:

Address:

Office Phone:

Fax:

Email:

6. OTHER PROVISIONS: Nothing in this MOA is intended to conflict with current law or regulation or the directives of the sponsoring Federal Agency. If a term of this MOA is inconsistent with such authority, then that term shall be invalid, but the remaining terms and conditions of this MOA shall remain in full force and effect. This MOA does not result in transfer of funds or other financial obligations between the parties.

7. EFFECTIVE DATE: The terms of this MOA shall become effective on DATE.

8. MODIFICATION: This MOA may be modified upon the mutual written consent of the parties.

9. TERMINATION: The terms of this MOA, as modified with the consent of both parties, shall remain in effect until ENTER CONTRACT TERMINATION DATE, or upon written agreement of the parties. Termination of the MOA, by either party, shall concurrently result in the termination of access to classified information by the contractor in support of the applicable contract. The MOA may be extended by mutual written agreement of the parties and upon presentation to the signatories, or their successor in function, of a contract modification extending the terms of the contract. Either party upon 30 days written notice to the other party may terminate this MOA.

10. APPROVED BY:

DESIGNATED FEDERAL POC

TITLE

APPROPRIATE

CONTRACTOR FSO OR

OTHER

ORGANIZATION CORPORATE OFFICER

DATE DATE

Addendum: DD Form 254

Appendix 9

Definitions

A. *Access:* means the ability or opportunity to gain knowledge of classified information.

B. *Agency:* means any ‘‘Executive agency,’’ as defined in 5 U.S.C. 105; any ‘‘Military department’’ as defined in 5 U.S.C. 102; and any other entity within the executive branch that comes into the possession of classified information.

C. *Authorized holder:* of classified information means anyone who satisfies the conditions for access stated in E.O. 13526

D. *Authorized person:* means a persons who has a favorable determination of eligibility for access to classified information, has signed an approved nondisclosure agreement, and has a need-to-know

E. *Classification:* means the act or process by which information is determined to be classified information.

F. *Classification guidance:* means any instruction or source that prescribes the classification of specific information.

G. *Classification guide:* means a documentary form of classification guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

H. *Classification management:* means the life-cycle management of classified national security information from original classification to declassification.

I. *Classified national security information’’ or ‘‘classified information’’:* means information that has been determined pursuant to Executive Order 13526 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

J. *Closed Storage:* for the purpose of this directive, closed storage means the securing of classified information in an approved security container when unattended.

K. *Compromise:* means any occurrence that results or may likely result in unauthorized persons gaining access to classified information.

L. *Confidential:* level of classification applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

M. *Damage to the national security:* means harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, taking into consideration such aspects of the information as the sensitivity, value, utility, and provenance of that information.

N. *Declassification:* means the authorized change in the status of information from classified information to unclassified information.

O. *Derivative classification:* means the incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

P. *Information:* means any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics that is owned by, is produced by or for, or is under the control of the United States Government.

Q. *Information security:* means the system of policies, procedures, and requirements established under the authority of E.O. 13526, to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to the national security.

R. *Infraction:* means any knowing, willful, or negligent action contrary to the requirements of this order or its implementing directives that does not constitute a ‘‘violation,’’ as defined below.

S. *Intelligence:* includes foreign intelligence and counterintelligence as defined by Executive Order 12333 of December 4, 1981, as amended, or by a successor order.

T. *Intelligence activities:* means all activities that elements of the Intelligence Community are authorized to conduct pursuant to law or Executive Order 12333, as amended, or a successor order.

U. *Intelligence Community:* means an element or agency of the U.S. Government identified in or designated pursuant to section 3(4) of the National Security Act of 1947, as amended, or section 3.5(h) of Executive Order 12333, as amended.

V. *Local government:* means (A) a county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under State law), regional or interstate government entity, or agency or instrumentality of a local government; (B) an Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation; and (C) a rural community, unincorporated town or village, or other public entity.

W. *National security:* means the national defense or foreign relations of the United States.

X. *Need-to-know:* means a determination within the executive branch in accordance with directives issued pursuant to Executive Order 13526 that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

Y. *Open storage area:* means an area constructed in accordance with §2001.53 of 32 C.F.R. Part 2001 and this directive and authorized by the agency head for open storage of classified information. For the purposes of this directive, an open storage area also means an area that has been approved for open storage only to accommodate classified connectivity associated with the deployment of a classified information system, e.g., HSDN. In this instance, open storage refers only to the classified systems connectivity while all other form of media containing classified information is maintained in closed storage.

Z. *Original classification:* means an initial determination that information requires, in the interest of the national security, protection against unauthorized disclosure.

AA. *Original classification authority:* means an individual authorized in writing, either by the President, the Vice President, or by agency heads or other officials designated by the President, to classify information in the first instance.

BB. *Safeguarding:* means measures and controls that are prescribed to protect classified information.

CC. *Secret:* level of classification applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

DD. *Security-in-depth:* means a determination by the agency head that a facility's security program consists of layered and complementary security controls sufficient to deter and detect unauthorized entry and movement within the facility. Examples include, but are not limited to, use of perimeter fences, employee and visitor access controls, use of an Intrusion Detection System (IDS), random guard patrols throughout the facility during nonworking hours, closed circuit video monitoring or other safeguards that further solidify the security of an area or mitigate potential vulnerabilities.

EE. *Sensitive Compartmented Information (SCI):* means classified national intelligence concerning or derived from intelligence sources, methods, or analytical processes that is required to be protected within formal access control systems established and overseen by the Director of National Intelligence.

EE. *State:* The term ''State'' means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States.

FF. *Supplemental controls:* means prescribed procedures of systems that provide security control measures designed to augment the physical protection of classified information. Examples of supplemental controls include intrusion detection systems, periodic inspections of security containers or areas, and security-in-depth.

GG. *Top Secret:* level of classification applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

HH. *Unauthorized disclosure:* means a communication or physical transfer of classified information to an unauthorized recipient.

II. *U.S. entity* includes:

(1) State, local, or tribal governments;

(2) State, local, and tribal law enforcement and firefighting entities;

(3) public health and medical entities;

(4) regional, state, local, and tribal emergency management entities, including State Adjutants General and other appropriate public safety entities; or

(5) private sector entities serving as part of the nation's Critical Infrastructure/Key Resources.

JJ. *Violation* means:

(1) any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information;

(2) any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of this order, its implementing directives; or

(3) any knowing, willful, or negligent action to create or continue a special access program contrary to the requirements of this order.

KK. *Waiver*: For the purposes of this directive, waiver means a deviation, normally temporary in nature, from established requirements.