CLASSIFIED NATIONAL SECURITY INFORMATION PROGRAM

1. **PURPOSE:** This notice amends the Department of Veterans Affairs (VA) Directive 0734, Classified National Security Information (CNSI) Program, dated July 7, 2017. An accompanying VA Handbook to provide guidance outlining the procedures and processes for the execution and administration of VA CNSI and Sensitive Compartmented Information (SCI) programs will be forthcoming.

2. **POLICY:** The amended guidance will outline the current structure, activities, and processes for the CNSI and SCI related to the physical security of VA SCI facilities (SCIF), authorized access and visitor control procedures, and technical security. The VA Special Security Officer (SSO) must be the primary point of contact for matters related to SCI. SCIFs must be designated as restricted areas.

    a. Access to SCIFs, CNSI, or SCI, must be based on applicable security clearances, need-to-know, and subject to technical security measures. Personnel who work in or have unescorted access to a SCIF must be indoctrinated for the compartments that are discussed, processed, or stored within the facility. Non-SCI-indoctrinated personnel must be escorted by an SCI-indoctrinated employee and must comply with SCIF visitor standards. Escorts must secure all SCI material (including SCI information displayed on information systems) and cease any SCI discussions. Foreign nationals are not permitted to access any VA SCIF, unless approved in writing. See subsection f of this part.

    b. The Office of Operations, Security and Preparedness (007) (OSP) shall assess all current and future Top Secret SCI VA positions to validate an employee's CNSI need-to-know. Only personnel with continuous and ongoing access to classified information, or with legal or policy requirements, shall be approved for SCI eligibility or access. Intermittent or short duration access to classified information and/or SCIF will be managed on a case-by-case basis with temporary escorted access.

    c. Operations security (OPSEC) principles must be considered and implemented for protecting the operations, activities, and security of SCIFs. SCIF locations (complete address) and facility identification as a SCIF must be protected at a minimum as CONTROLLED UNCLASSIFIED INFORMATION. Drawings or diagrams identified as a SCIF must not be posted on an UNCLASSIFIED website or transmitted over the internet without encryption.

    d. All CNSI or SCI material must be stored in a GSA-approved security container in an accredited facility. Secured working areas (SWAs) may be accredited and used for handling, discussing, and processing collateral (non-SCI) CNSI.

    e. The SSO, or designee, must manage a system of written end-of-day security checks to properly protect all classified materials and to ensure that the SCIF is secured. These checks must include a completed Standard Form (SF) 701, "Activity Security Checklist," to record end-of-day internal security checks and

SF 702, “Security Container Check Sheet,” to record the security checks of the SCIF door, vaults, and containers.

f. The SSO is the primary POC for verification of SCI accesses. Use of the approved clearance verification system (i.e., Defense Information System for Security (DISS) or the IC Security Clearance Repository (Scattered Castles)) is the preferred method for verification of clearances and accesses.

g. Foreign National visitor access to U.S.-controlled SCIFs may only be permitted given written approval by the Head of an Intelligence Community (IC) Element, designee, or appropriate IC authority and based on operational need.

h. Portable electronic devices (PEDs) are prohibited inside SCIFs and while reviewing or discussing CNSI or SCI. Local SCIF policies may require storage of PEDs at a distance from the SCIF. Properly configured government-furnished equipment must be expressly authorized, in writing, by the SSO for use within the SCIF.

3. **RESPONSIBLE OFFICE:** Office of Operations, Security and Preparedness (007), Office of Emergency Management and Resilience (07A).

4. **RELATED DIRECTIVE and/or HANDBOOK:** VA Directive 0734, Classified National Security Information (CNSI) Program, dated July 7, 2017.

5. **RECISSION(s):** This notice will be rescinded, and guidance incorporated into VA Directive 0734, Classified National Security Information (CNSI) Program, no later than one year after the date of publication.

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/s/
Ian M. Dinesen
Acting Assistant Secretary for
Operations, Security and Preparedness

DISTRIBUTION: Electronic Only