COVID-19 NISP Guidance

March 30, 2020

Please send all NISP inquiries related to COVID-19 impacts to your assigned Industrial Security Representative.

Facility Clearance (FCL) Processing: FCL requests will continue to be processed. However, Facility Clearance Inquiries (Option 3 of the DCSA Knowledge Center) will be suspended until further notice. Status inquiries can be obtained by leaving a detailed voicemail message on the Knowledge Center voice mail or sending a detailed email to the Facility Clearance Branch (FCB) mailbox at dcsa.fcb@mail.mil. Please include your Facility CAGE Code and name for all status inquiries. All messages will be returned within one day.

Personnel Security: Contractors are encouraged to continue to utilize the Knowledge Center to resolve system lockouts for JPAS, DISS, and NISS. Please be mindful of the menu options, which may have changed, and follow the instructions; as applicable.

In conjunction with COVID-19 measures, the DoD CAF Call Center is temporarily suspending its phone service. It's encouraged to submit questions/inquiries to the DoD CAF group mailbox at whs.meade.dodcaf.mbx.dodcaf-callcenter@mail.mil. Please place as much detail as possible. An agent will follow up soonest via email in the order in which the request was received.

Administrative Debriefs: Cleared contractors under DoD Cognizance may until further notice conduct administrative debriefs of cleared personnel leaving employment when the employee is not physically available. The administrative debrief may be conducted via virtual means (telephone, email, text, video teleconference, etc.) with the exception if discussion of classified material is required. The FSO must attempt to obtain written acknowledgement from the subject being debriefed and retain as a record within your local security files. Once debriefed, the system of record, must be updated to reflect the action. For personnel with SAP or SCI access follow guidance provided by your government customer.

Refresher Training: The NISPOM requires training to be conducted annually, which directs that training must be conducted once during each calendar year, unless specifically identified in the training requirement or by the Government Contracting Activity. Until further notice, cleared contractors may adjust scheduled NISPOM refresher training based on employee availability and status. Cleared contractors will have a plan in place to ensure that refresher training is resumed, and all overdue training is completed within 60-days of returning to normal operations. This does not preclude the training requirements for personnel that remain on duty and the training that is required to perform the security related task; for example derivative classification which must be current for all derivative classifiers. Cleared contractor employees not in current work status (furloughed or not in pay status) should be removed from access in JPAS and as such, do not require training to be maintained until they return to work.

Security Reviews: Due to the COVID-19 national emergency, DCSA is suspending all ESVAs and on-site activities until further notice. Facilities scheduled to receive an ESVA will instead be

contacted virtually by their Industrial Security Representative (ISR) who will conduct a Continuous Monitoring Engagement. Please contact your assigned ISR with any questions.

Safeguarding: All classified information should be properly secured in accordance with NISPOM requirements and approved safeguarding procedures prior to office closure. This includes areas implementing mandatory quarantines. The contractor must contact their ISR if they encounter any issues following office closure.

End-of-Day Checks: End-of-day checks on security containers and secure areas are not waived. The contractor is responsible for ensuring classified material remains appropriately secured. If security containers are located in an open work space (example: hallways) or in a secure space that has been opened (example: closed area), end of day checks need to be conducted. However, during the COVID-19 pandemic, if security containers are in a secure area that was **not** opened, the space does **not** need to be opened simply to conduct end-of-day checks on the container. If the office is closed and the contractor can confirm that no one entered the office space, there is **no** need for an authorized employee go in and check the containers or secure areas and perform end-of-day-checks.

DCSA Approved Closed Areas: If a DCSA-approved secure space safeguards TOP SECRET information, all efforts should be made to continue to leverage dual authentication while mitigating the risk of virus transmission (example: latex gloves, keypad sanitization, etc.). However, if the contractor's access cards allow for identification of whoever is entering the space and the contractor can ensure physical control of all access cards by the respective owners then the contractor may decide to temporarily suspend the need for a PIN. The contractor should identify a specific length of time this would be suspended, not "until further notice" (example - two weeks at a time), and reevaluate circumstances at the conclusion of that time period. The contractor should also identify additional accountability requirements and checks for the access cards to manage the risk posed by removing the dual authentication. The contractor should notify their ISR that they are implementing temporary measures and keep DCSA informed of the status and any issues.

Special Access Program Facilities (SAPF): In accordance with DoDM 5205.07-V3 Physical Security: DoD Component special access program central offices (SAPCOs) with cognizant authority and oversight authority over SAPs grants waivers to the standards stipulated in this volume based on a risk assessment and operational requirements. DCSA does not authorize or accredit Special Access Program Facilities (SAPF) regardless if DCSA is the cognizant security office or if there is an approved carve-out provision relieving DCSA of the industrial security oversight role. Accreditation of SAPFs is usually accomplished by the government program security officer (PSO). Approval of changes to the standards for SAPFs should be coordinated to the cognizant authority special access program central office (CA SAPCO) through the appropriate PSO.

Transmission: Use of FedEx to transmit classified material requires prior approval from DCSA (NISPOM 5-403(e)). Additionally, DCSA has received notification of instances where FedEx is delivering packages without obtaining required signatures. If DCSA has approved a facility to use FedEx to transmit classified material and the facility has plans to do so during the COVID-19 pandemic, the facility must:

- Validate with FedEx that it will be delivered in accordance with requirements (i.e. only delivered after a signature is obtained)
- Validate that the receiving facility is open and an appropriately cleared individual with a need-to-know is available to receive the package.

If a contractor is closing their office, they should notify their GCA(s), prime contractor(s), and ISR to pre-empt any transmission of classified information to their office.

Classified material should **not** be delivered and left unattended. Any instances of classified material being delivered or received inappropriately is considered a security violation and must be processed as such.

Authorized Information Systems: DCSA will extend all Authorizations to Operate (ATOs) expiring before April 18, 2020 for an additional 90 days. This will allow DCSA to work with Industry to ensure operations to support the warfighter and classified programs are sustained. The following guidance from the DCSA Assessment and Authorization Process Manual (DAAPM) is also provided:

Assess and Authorize Activities (DAAPM 2.1): Security Control Assessment (SCA) activity will continue to occur. The onsite portion of the SCA activity will be delayed, deferred, or rescheduled. Documenting evidence of security and validation requirements remain unchanged; only the execution of onsite activity will change temporarily.

Audit Variances (DAAPM 12): During periods of system inactivity (e.g., hibernation) or when a facility plans to stop work for an extended period of time (e.g., holiday shutdowns), an audit variance may be authorized. Periods of hibernation will not exceed 180 days without Regional Authorizing Official approval. When requesting an audit variance, Industry must have a Standard Operating Procedure (SOP) in place that specifies how the system will be protected during a dormant state. The SOP will include a process for protecting the system through the use of physical security controls (e.g., seals, locks, alarms, and GSA-approved containers), technical controls (e.g., whole disk encryption, disabled accounts, and audit logs), and immediate patching/ updates upon return to service. The audit variance will be authorized via the security plan (i.e., added as a supporting artifact). Industry is required to maintain a log of audit variance activities on-site. Audit variance documentation will be assessed during the ESVA and other engagement activities (e.g., Advise & Assist visits, periodic communications, etc.).