DEPARTMENT OF DEFENSE
DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY
QUANTICO, VA 22134-6801

# INDUSTRIAL SECURITY LETTER

**Disclaimer:** ***The contents of this document do not have the force and effect of law and are not meant to bind the public in any way. This document is intended only to provide clarity to the public regarding existing requirements under the law or departmental policies.***

Industrial security letters (ISLs) are issued as necessary to inform cleared contractors, government contracting activities, and DoD Components of developments relating to the National Industrial Security Program (NISP). ISLs are provided for information and clarification of existing policy and requirements. ISLs pertain only to those entities for whom the Department of Defense is the Cognizant Security Agency. For inquiries about specific information in ISLs, or suggestions for new ISLs, please contact your local DCSA industrial security field office.

**ISL 2024-01** **January 25, 2024**

**32 CFR 117.18, Information Systems.** DCSA authorizes classified information systems for cleared contractors when required by the government contracting activity (GCA). This ISL provides clarity on the process for DCSA to verify GCA authorization for a contractor's use of commercial cloud services (CCS) in the performance of a classified contract, as required by the Defense Federal Acquisition Regulation Supplement (DFARS).

**Commercial Cloud Services Authorization.** The DCSA NISP Authorizing Official (NAO) may authorize Impact Level (IL) 6 CCS under one of the methods below to verify the contract requirement.

1. On the DD Form 254, "Contract Security Classification Specification," block 11c ("Receive, Store, and Generate Classified Information or Material," is checked, and details on the use of IL6 CCS pursuant to contract-specific performance requirements are provided in item 13.

2. If this information is not provided on the DD Form 254, the contractor may verify to DCSA that DFARS clause 252.239.7010, "Cloud Computing Services, is included in each contract for which IL6 CCS are required.

3. If the contractor initially indicated in the solicitation that it did not anticipate using CCS in the performance of the contract, but later decides otherwise, DFARS clause 252.239-7010 states that the contractor "shall obtain approval from the Contracting Officer prior to utilizing cloud computing services in performance of the contract." Proof of the contracting officer's approval may be accepted in a variety of forms, to include an email from the contracting officer or empowered official.

As a reminder, contracts that include DFARS Clause 252.239.7010 establish a requirement for the contractor to comply with the Defense Information Systems Agency (DISA) Cloud Computing Security Requirements Guide. DCSA will determine if the CCS proposed for use by the contractor meet DISA's provisional authorization requirements as described in the guide.

**Resources.** For more information, contractors may email the NISP Cybersecurity Office at dcsa.quantico.hq.mbx.nao@mail.mil.

**Definition**. Cloud computing: DFARS 252.239.7009 defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This includes other commercial terms, such as on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. It also includes commercial offerings for software-as-a-service, infrastructure-as-a-service, and platform-as-a-service."