DEPARTMENT OF DEFENSE • DEFENSE SECURITY SERVICE

INDUSTRIAL SECURITY LETTER

ISL 2011-02 **April 12, 2011**

The National Industrial Security Program Operating Manual (NISPOM) paragraphs to which these articles pertain are indicated in parentheses.

(2-208) Acceptable Proof of Citizenship

In December 2009, the government of Puerto Rico enacted a new law aimed at strengthening the issuance and usage of birth certificates to combat fraud and protect the identity and credit of all people born in Puerto Rico. The new law was based on collaboration with the U.S. Department of State and the U.S. Department of Homeland Security.

On July 1, 2010, Puerto Rico began issuing new birth certificates incorporating technology to limit the possibility of document forgery. The government of Puerto Rico extended the validity of expiring Puerto Rico birth certificates through October 30, 2010, as a transition period.

Contractors verifying citizenship of applicants who use a Puerto Rican birth certificate as proof of citizenship must verify that the birth certificate was issued on or after July 1, 2010. There is no requirement to re-verify citizenship for employees who used a birth certificate from Puerto Rico as proof of U.S. citizenship prior to October 30, 2010.

For additional information, visit the Puerto Rico Federal Affairs Administration link below: http://www.prfaa.com/index.asp

(2-303c.(2)) Special Security Agreement (SSA)

Communications Security (COMSEC) and Proscribed Information

Question: In the context of National Industrial Security Program Operating Manual (NISPOM) paragraph 2-303c.(2), when is COMSEC material considered proscribed information?

Answer: All COMSEC material is proscribed information except for Controlled Cryptographic Items when unkeyed or utilized with unclassified keys.

Background:

In accordance with NISPOM paragraph 2-303c.(2), companies cleared under Special Security Agreements (SSAs) require National Interest Determinations (NIDs) in order to perform on contracts requiring access to proscribed information. The current version of the NISPOM defines the COMSEC category of proscribed information as "COMSEC, except classified keys used for data transfer."

Unfortunately, this definition is ambiguous and has created confusion. To some contractor personnel and government officials, the current wording suggests that all COMSEC hardware (even unclassified Controlled Cryptographic Items) is proscribed information while even the most sensitive classified keys are not. This is not the intended interpretation.

To address the ambiguity and to resolve any confusion, the Department of Defense (DoD) has issued the following revised definition of proscribed information to DoD Government Contracting Activities and to the 23 non-DoD agencies receiving DoD industrial security services. This clarification reflects current DoD policies and practices and will be incorporated into the next revision to the NISPOM.

> *Proscribed information includes Top Secret (TS); COMSEC material, excluding Controlled Cryptographic Items when unkeyed or utilized with unclassified keys; Restricted Data (RD); Special Access Program (SAP); and Sensitive Compartmented Information (SCI). Access to the proscribed information in this subparagraph shall not be granted without the approval of the agency with control jurisdiction (e.g., National Security Agency (NSA) for COMSEC, whether the COMSEC is proscribed information or not; the Office of the Director of National Intelligence (ODNI) for SCI; and Department of Energy (DOE) for RD) in accordance with its policies.*

NSA will (as stated in NISPOM 9-401) continue to establish specific requirements for the management and safeguarding of COMSEC materials in industry. In addition, NSA approval will be required before access to COMSEC can be granted, regardless of whether the COMSEC information is proscribed or classified information and whether or not there is a Foreign Ownership, Control or Influence mitigation agreement in place.