



INDUSTRIAL SECURITY

LETTER

Industrial Security letters are issued periodically to inform cleared Contractors, User Agencies and DoD Activities of developments relating to industrial security. The contents of these letters are for information and clarification of existing policy and requirements. Suggestions for Industrial Security Letters are appreciated and should be submitted to the local Defense Security Service (DSS) cognizant industrial security office. Articles and ideas contributed will become the property of DSS. Inquiries concerning specific information in Industrial Security Letters should be addressed to the cognizant DSS industrial security office.

ISL 2009-01

March 5, 2009

This Industrial Security Letter (ISL) pertains to: (1) the Defense Security Service (DSS) Office of Designated Approving Authority (ODAA) “Manual for the Certification and Accreditation of Classified Systems under the National Industrial Security Program Operating Manual (NISPOM),” hereafter referred to as the “Manual”; and (2) the DSS ODAA “Standardization of Baseline Technical Security Configurations,” hereafter referred to as the “Baseline Standards.”

The purpose of this ISL is to establish appropriate uniformity, consistency, and standardization of security safeguards for contractor information systems (IS) used to process classified information. For some time, representatives of cleared contractors have asked DSS to clarify the safeguarding standards used to make a determination that an IS is eligible for accreditation. DSS agrees that it would be a benefit to contractors, and to DSS, to provide as much clarity as possible regarding the DSS accreditation process and requirements. The Manual and Baseline Standards are both published in an effort to provide cleared contractors with clear expectations about how DSS will accomplish its accreditation responsibilities.

The Manual and the Baseline Standards describe the baseline set of safeguards that DSS will apply when making an accreditation decision. DSS recognizes that the safeguards found in these documents will not all apply to every IS. DSS will fully review and consider the acceptability of deviations from the safeguards described in these documents on a case-by-case basis. Both the Manual and the Baseline Standards will be updated and published by DSS as the standards upon which they are based are revised.

The guidance in this ISL is effective immediately. Contractors may continue to operate IS that were accredited and approved to process classified information under previous guidelines. Contractors should use the guidelines found in the Manual and Baseline Standards for any new IS submitted to DSS for accreditation and for any IS to be considered for reaccreditation.

1. ODAA Manual (NISPOM 8-101a, 8-202, 8-610a(1)(b)(3))

Use of the Manual will support contractor compliance with the NISPOM. The Manual sets forth guidance for contractors to use in developing their system security plans (SSPs) and continuous certification and accreditation requirements. The Manual implements and conforms to NISPOM requirements, and is based on other Federal standards* that apply to national security systems used by Government and contractors. Use of, and adherence to, the Manual will facilitate the DSS review of SSPs and IS certifications.

The Manual is available on the DSS website: www.dss.mil.

* These standards include: Department of Defense (DoD), National Security Agency (NSA), Defense Information System Agency (DISA), National Institute of Standards and Technology (NIST), and the Committee on National Security Systems (CNSS).

The CNSS (see National Security Directive Number 42, and Executive Order (EO) 13231, October 16, 2001) is chaired by the Department of Defense and is charged with setting national policy, operational procedures and guidance for National Security Systems (NSS). The CNSS goal was a convergence of standards for the DoD, Intelligence, and civilian communities into one common, consistent process with one set of common standards for the federal security authorization process (i.e., certification and accreditation). Contractor IS used to process classified information are defined as national security systems (NSS) per the Federal Information Security Management Act (FISMA) of 2002 (44 U.S.C. §3541, *et seq.*, which refers to the definition of NSS at 44 U.S.C. §3532(b)(2)).

By FISMA definition, NSS are those that are used or operated by an agency or by a contractor of an agency, or another organization on behalf of the agency, the function, operation, or use of which involves intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment that is an integral part of a weapon system, or are protected at all times by procedures established for information that have been specifically authorized under criteria established by an EO or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

The CNSS is also currently drafting the set of standards for NSS in draft CNSS Instruction 1253, "Security Control Catalog for National Security Systems". These CNSS security standards and guidelines are integrated into a risk management framework that promotes the concept of "near real-time risk management" based on continuous monitoring of information systems. As contractor IS used to process classified information are considered to be NSS, DSS anticipates that these CNSS standards will form the basis of any future revisions to NISPOM requirements pertaining to IS security.

2. ODAA Baseline Standards (NISPOM 8-101a, 8-202, Section 6 of Chapter 8)

In accordance with its National Industrial Security Program oversight responsibilities, and as provided for in NISPOM 8-202, DSS has established an approved set of technical safeguards that DSS will apply in making a decision to accredit an IS. These technical safeguards are set forth in the Baseline Standards. The technical configurations prescribed in the Baseline Standards conform to NISPOM protection requirements (Section 6 of Chapter 8), as well as to Federal standards that apply to Government systems.

Using the baseline set of safeguards in the Baseline Standards will assist contractors in meeting their requirement to select, test, certify and document that a baseline of technical security controls has been implemented.

Contractor application of the safeguards in the Baseline Standards will facilitate the DSS decision to accredit an IS; that is, for DSS to take a risk-management approach to authorize an IS to operate in accordance with a specific set of baseline security settings for a specific IS in a specific environment and explicitly accepting the residual risk.

The Baseline Standards is available on the DSS website: www.dss.mil