MEMORANDUM FOR DISTRIBUTION

Subj: CLASS DEVIATION-EXEMPTION FROM LIMITATIONS ON PROCUREMENT OF FOREIGN INFORMATION TECHNOLOGY THAT IS A COMMERCIAL ITEM

Encl: (1) DPAP memo dtd May 18, 2004

Enclosure (1) is provided for your immediate implementation and action, as appropriate. The Director of Defense Procurement and Acquisition Policy has authorized a class deviation from the Defense Federal Acquisition Regulation Supplement (DFARS) requirements to apply the Buy American Act or Balance of Payments Program to the acquisition of information technology that is a commercial item. The deviation authorizes contracting officers to not use the DFARS provisions and clauses, 252.225-7000, 252.225-7001, 252.225-7035, and 252.225-7036 when using fiscal year 2004 funds to acquire information technology that is a commercial item.

This class deviation is effective immediately, and remains in effect until incorporated in the DFARS or until otherwise rescinded.

Please forward the enclosed memorandum to appropriate contracting personnel.

M. J. Landgraf
Chief of Staff/Policy
for DASN (ACQ MGMT)

Distribution:
See next page
Subject: CLASS DEVIATION-EXEMPTION FROM LIMITATIONS ON PROCUREMENT OF FOREIGN INFORMATION TECHNOLOGY THAT IS A COMMERCIAL ITEM

DISTRIBUTION:
NAVAIRSYSCOM (2.0)
NAVFACENGCOM (ACQ 02)
NAVSEASYSCOM (02)
NAVSUPSYSCOM (02)
SPAWARSYSCOM (02)
MARCORSYSCOM (CT)
NAVICP (02)
ONR (02)
CMC (LB)
MSC (N10)
SSP (SPN)
MEMORANDUM FOR DIRECTORS OF DEFENSE AGENCIES
DEPUTY ASSISTANT SECRETARY OF THE ARMY,
(POLICY AND PROCUREMENT), ASA(ALT)
DEPUTY ASSISTANT SECRETARY OF THE NAVY
(ACQUISITION MANAGEMENT), ASN(RDA)
DEPUTY ASSISTANT SECRETARY OF THE AIR FORCE
(CONTRACTING), SAF/AQC
DIRECTOR, DEFENSE CONTRACT MANAGEMENT AGENCY
EXECUTIVE DIRECTOR, ACQUISITION, TECHNOLOGY AND
SUPPLY DIRECTORATE (DLA)

SUBJECT: Class Deviation—Exemption from Limitations on Procurement of Foreign
Information Technology that is a Commercial Item

When using fiscal year 2004 funds to acquire information technology that is a
commercial item, do not use any of the following Defense Federal Acquisition
Regulation Supplement (DFARS) provisions and clauses as prescribed at DFARS
225.1101(1), (2), (9), and (10) or the associated FAR clauses which they otherwise
replace:

- 252.225-7000, Buy American Act—Balance of Payments Program
  Certificate.
- 252.225-7001, Buy American Act and Balance of Payments Program.
- 252.225-7035, Buy American Act—Free Trade Agreements—Balance of
  Payments Program Certificate.
- 252.225-7036, Buy American Act—Free Trade Agreements—Balance of
  Payments Program.

The Buy American Act does not apply to these acquisitions of foreign information
technology because Section 535 of Division F of the Consolidated Appropriations Act,
2004 (Pub. L. 108-199) provides exemption (Atch 1). “Information technology” is
defined at 40 U.S.C. 11101 (Atch 2).
When applicable, continue to use the Trade Agreements provision and clause at 252.225-7020 and 252.225-7021, as prescribed at 225.1101(5) and (6).

This class deviation is effective upon signature, and remains in effect until incorporated in the DFARS or until otherwise rescinded.

\[signature\]

Deidre A. Lee
Director, Defense Procurement
and Acquisition Policy

Attachments:
As stated

c c:
DSMC, Ft. Belvoir
§ 1101.02 Application to national security systems

1101.02(a) National Security System (NSS) Information Technology (IT) Systems

A national security system (NSS) information technology (IT) system is a computer-based system that automates or otherwise aids in the processing, storage, retrieval, manipulation, or dissemination of information that falls within any one or more of the following categories:

1. Systems that support national defense.
2. Systems that support national security.
3. Systems that support national intelligence.

1101.02(b) NSS IT Systems

An NSS IT system is an IT system that is part of a national security system and is used to support national security activities. These include systems that:

1. Collect, store, process, or transmit information that is used to support national security.
2. Support the operation of national security systems.
3. Provide security services to other systems that support national security.

1101.02(c) NSDD

The National Security Decision Directive (NSDD) is a policy guidance document issued by the President's Office in accordance with Executive Order 12333. It establishes the policies and procedures for the protection of national security systems, including the development, acquisition, and operation of NSS IT systems.

1101.02(d) NSS Security

The security of NSS IT systems is critical to the protection of the nation's security interests. It is the responsibility of the owner or operator of an NSS IT system to ensure that the system is adequately secured to protect against unauthorized access, modification, or disclosure of information.

1101.02(e) NSS IT Security

NSS IT security includes measures to protect NSS IT systems from unauthorized access, modification, or disclosure. These measures may include, but are not limited to, physical security, network security, system security, and personnel security.

1101.02(f) NSS IT Security Controls

NSS IT security controls are the specific actions taken to protect NSS IT systems. These controls may include technical controls, management controls, and physical security controls.

1101.02(g) NSS IT Security Plan

An NSS IT security plan is a document that outlines the security measures and practices to be implemented to protect NSS IT systems. The plan is reviewed and updated on a regular basis to ensure that it remains effective.

1101.02(h) NSS IT Security Training

NSS IT security training is provided to personnel who have access to or work with NSS IT systems. The training includes instruction on security policies, procedures, and best practices.

1101.02(i) NSS IT Security Tests and Evaluations

NSS IT security tests and evaluations are conducted to assess the effectiveness of NSS IT security measures. These tests may include penetration testing, vulnerability assessments, and other security analyses.

1101.02(j) NSS IT Security Audits

NSS IT security audits are conducted to ensure that NSS IT systems are being operated in accordance with security policies and procedures. The audits may be conducted internally by the owner or operator of the system or by an independent third party.

1101.02(k) NSS IT Security Incident Response

NSS IT security incident response is the process of identifying, containing, and recovering from security incidents that affect NSS IT systems. This includes the development of incident response plans and procedures.

1101.02(l) NSS IT Security Incident Management

NSS IT security incident management is the process of managing and reporting security incidents that occur within NSS IT systems. This includes the development of incident management plans and procedures.

1101.02(m) NSS IT Security Incident Reporting

NSS IT security incident reporting is the process of reporting security incidents to the appropriate authorities. This includes the development of incident reporting procedures and the establishment of a reporting chain of command.

1101.02(n) NSS IT Security Incident Documentation

NSS IT security incident documentation is the process of recording and maintaining information about security incidents. This includes the development of incident documentation procedures and the establishment of a documentation chain of command.

1101.02(o) NSS IT Security Incident Analysis

NSS IT security incident analysis is the process of analyzing security incidents to determine the causes and effects of the incidents. This includes the development of incident analysis procedures and the establishment of an analysis chain of command.

1101.02(p) NSS IT Security Incident Mitigation

NSS IT security incident mitigation is the process of taking action to prevent the occurrence of future security incidents. This includes the development of incident mitigation procedures and the establishment of a mitigation chain of command.

1101.02(q) NSS IT Security Incident Recovery

NSS IT security incident recovery is the process of restoring NSS IT systems to normal operation after a security incident. This includes the development of incident recovery procedures and the establishment of a recovery chain of command.

1101.02(r) NSS IT Security Incident Lessons Learned

NSS IT security incident lessons learned are the process of identifying and documenting the lessons learned from security incidents. This includes the development of incident lessons learned procedures and the establishment of a lessons learned chain of command.

1101.02(s) NSS IT Security Incident Reporting Requirements

NSS IT security incident reporting requirements are the requirements that must be met when reporting security incidents. These requirements may include the development of incident reporting guidelines and the establishment of a reporting chain of command.

1101.02(t) NSS IT Security Incident Reporting Guidelines

NSS IT security incident reporting guidelines are the guidelines that must be followed when reporting security incidents. These guidelines may include the development of incident reporting requirements and the establishment of a reporting chain of command.

1101.02(u) NSS IT Security Incident Reporting Chain of Command

NSS IT security incident reporting chain of command is the chain of command that must be followed when reporting security incidents. This includes the development of incident reporting chains and the establishment of a reporting chain of command.

1101.02(v) NSS IT Security Incident Reporting Chain of Command Requirements

NSS IT security incident reporting chain of command requirements are the requirements that must be met when establishing incident reporting chains. These requirements may include the development of incident reporting chains and the establishment of a reporting chain of command.

1101.02(w) NSS IT Security Incident Reporting Chain of Command Guidelines

NSS IT security incident reporting chain of command guidelines are the guidelines that must be followed when establishing incident reporting chains. These guidelines may include the development of incident reporting chains and the establishment of a reporting chain of command.

1101.02(x) NSS IT Security Incident Reporting Chain of Command Chain of Command

NSS IT security incident reporting chain of command chain of command is the chain of command that must be followed when establishing incident reporting chains. This includes the development of incident reporting chains and the establishment of a reporting chain of command.

1101.02(y) NSS IT Security Incident Reporting Chain of Command Requirements

NSS IT security incident reporting chain of command requirements are the requirements that must be met when establishing incident reporting chains. These requirements may include the development of incident reporting chains and the establishment of a reporting chain of command.

1101.02(z) NSS IT Security Incident Reporting Chain of Command Guidelines

NSS IT security incident reporting chain of command guidelines are the guidelines that must be followed when establishing incident reporting chains. These guidelines may include the development of incident reporting chains and the establishment of a reporting chain of command.