Print

# U.S. Department of Energy
**Washington, D.C.**

# NOTICE

DOE N 205.2

Approved: 11/01/99
Expires: 06/01/00

**SUBJECT: FOREIGN NATIONAL ACCESS TO DOE CYBER SYSTEMS**

1. OBJECTIVE. To ensure foreign national access to DOE cyber systems continues to advance DOE program objectives while enforcing information access restrictions. DOE cyber systems include computers, networks, and associated servers, as well as data storage, switching, display, and control devices.

2. APPLICABILITY. This notice applies to all Departmental elements and DOE contractor and sub-contractor organizations which have access to DOE cyber systems. The Contractor Requirements Document (CRD) attached to this notice sets forth requirements that are applicable to such contracts and subcontracts.

3. REQUIREMENTS.

   a. Access by foreign nationals to DOE cyber systems must be approved by an official designated by the DOE site manager or Lead Program Secretarial Officer (LPSO) who is accountable for the approval decision. This approval must 1) identify the specific cyber system(s) to which access is granted and the anticipated time period of the access, and 2) must be based on a documented assessment of risks and an identification of access controls. The risk assessment, cyber system access controls, and approval must be included in the security plan required by DOE N 142.1, UNCLASSIFIED FOREIGN VISITS AND ASSIGNMENTS, or in other documentation, (e.g., the site's Cyber Security Program Plan, or a visit-specific plan), if the site is exempt from DOE N 142.1.

   b. DOE site managers and LPSOs must ensure access by foreign nationals to the cyber systems described in the approval is periodically audited consistent with the documented risk upon which approval is based.

   c. Non-resident foreign nationals from Sensitive Countries are not permitted access, from other than a DOE site or DOE contractor premise, to cyber systems

**Distribution:**
All Departmental Elements

**Initiated By:**
Office of Security and Emergency Operations

containing “Unclassified Controlled Nuclear Information (UCNI)” or “Naval Nuclear Propulsion Information (NNPI).” DOE site managers and LPSOs are responsible for ensuring that DOE networked systems containing UCNI or NNPI have protective measures to prevent unauthorized access.

BILL RICHARDSON
Secretary of Energy

**ATTACHMENT 1**
**CONTRACTOR REQUIREMENTS DOCUMENT**
**FOR DOE N 205.2**

The following requirements apply to contractors and subcontractors who have access to DOE cyber systems.

1. Access by foreign nationals to DOE cyber systems must be approved by a contractor official designated by senior contractor management who is accountable for the approval decision. This approval must 1) identify the specific cyber system(s) to which access is granted and the anticipated time period of the access, and 2) be based on a documented assessment of risk and an identification or access controls. The risk assessment, cyber system access controls, and approval must be included in the security plan required by DOE N 142.1, UNCLASSIFIED FOREIGN VISITS AND ASSIGNMENTS, or in other documentation, (e.g., the site's Cyber Security Program Plan, or a visit-specific plan), if the site is exempt from DOE N 142.1.

2. Access by foreign nationals must be periodically audited consistent with the documented risk upon which the approval is based.

3. Non-resident foreign nationals from Sensitive Countries are not permitted access, from other than a DOE site or DOE contractor premises, to cyber systems containing "Unclassified Controlled Nuclear Information (UCNI)" or "Naval Nuclear Propulsion Information (NNPI)." Contractors and subcontractors must ensure that DOE networked systems containing UCNI or NNPI have protective measures to prevent unauthorized access.