



# ORDER 205.2B

Title:	<b>FOREIGN NATIONAL ACCESS TO DOE CYBER SYSTEMS</b>
Owner:	Jerry Craig, Information Technology Division, Office of Institutional and Business Operations
Approving Official:	Thomas M. Torkos, Chief Operating Officer, Office of the Director  {signature} /s/ Thomas M. Torkos
Approval Date:	10/20/08
Last Reviewed Date:	10/20/08
Cancellation:	Order 205.2A, Foreign National Access to DOE Cyber Systems

## TABLE OF CONTENTS

1.	PURPOSE .....	2
2.	APPLICABILITY .....	2
3.	POLICY .....	2
4.	IMPLEMENTATION .....	2
5.	RESPONSIBILITIES.....	4
	a. Director, Information Technology Division.....	4
6.	REQUIREMENTS .....	4
7.	REFERENCES.....	4
8.	DEFINITIONS.....	4
9.	REVISION HISTORY .....	5

The most recent and official controlled hard copy version of this directive resides with NETL's Directives Coordinator.  
 An electronic version of the controlled directive has been placed on the NETL Intranet for employee use. Printed  
 hard copies of this electronic version are considered noncontrolled documents.

1. **PURPOSE**

- a. To set forth the requirements for providing access to cyber systems by foreign nationals.

2. **APPLICABILITY**

- a. This order applies to all NETL programs, operations, and employees.

3. **POLICY**

- a. It is the policy of NETL to abide by the requirements contained in the Under Secretary of Energy Program Cyber Security Plan; DOE Order 142.1, Classified Visits Involving Foreign Nationals; and DOE Order 142.3, Unclassified Foreign Visits and Assignments Program.

4. **IMPLEMENTATION**

- a. Cyber security must coordinate with the local Safeguards and Security Program to ensure that IT access by foreign nationals is integrated with the requirements of DOE Order 142.1, Classified Visits Involving Foreign Nationals, and DOE Order 142.3, Unclassified Foreign Visits and Assignments Program.

Information systems, devices, media, or equipment owned by, or in the possession of, a foreign national must be managed using isolated and contained principles and requirements per the following regulations:

- (1) The Office of the Under Secretary of Energy recognizes that some circumstances and conditions make it impossible to implement some or many cyber security requirements. The following foreign national known risk classifies as such:
  - (a) Remote access collaborators conducting business on behalf of DOE and/or accessing DOE-owned information and/or systems (e.g., foreign national scientists conducting research for a DOE laboratory).
- (2) The Office of the Under Secretary of Energy promotes an isolated and contained approach for mitigating the risk posed by these conditions. This approach is based on isolating devices and individuals from other DOE resources in a manner that minimizes the potential damage by containing the impact within an acceptable limit if damage were to occur. An example of the isolated and contained approach is where visitors are allowed to use personally owned devices within a DOE site, but are not allowed to connect those devices to DOE networks (or are granted Internet access only using adequate network segmentation and monitoring).

The most recent and official controlled hard copy version of this directive resides with NETL's Directives Coordinator. An electronic version of the controlled directive has been placed on the NETL Intranet for employee use. Printed hard copies of this electronic version are considered noncontrolled documents.

- (3) The designated approving authority (DAA) must determine the acceptable limit using accepted risk management principles.
- (4) NETL cyber security must:
  - (a) Document these conditions of non-compliance in the relevant system security plans (SSP(s));
  - (b) Ensure DAA approval of the residual risk posed by these conditions;
  - (c) Continuously reassess the potential impact of these conditions; and
  - (d) Ensure that the program cyber security plan's rules of behavior are understood and agreed to by individuals.
- (5) Foreign nationals must be screened prior to the access of NETL information systems. The categories for foreign nationals are as follows:
  - (a) General users must be screened to include a human resources background check and a national agency check.
  - (b) Privileged users must be screened to include a human resources background check and a national agency check with inquiries.
  - (c) Administrators must be screened to include a human resources background check and a national agency check with law and credit.
- (6) Foreign national privileged users and administrators may access DOE systems only from a DOE-managed facility.
- (7) Non-resident foreign nationals from sensitive countries may access DOE information systems containing unclassified controlled information (UCI) only from other DOE managed facilities.
- (8) Foreign nationals may not use non-DOE equipment to access UCI.
- (9) The cyber security team will ensure that encryption programs or algorithms in excess of 128 bits are not exported out of the United States in accordance with the requirements of 15 CFR 730-774, Bureau of Export Administration, Department of Commerce.
- (10) Foreign nationals may not bring their own encryption software for use on DOE-owned or managed systems.

5. **RESPONSIBILITIES**

a. Director, Information Technology Division

- (1) Ensures the requirements for this order are implemented.

6. **REQUIREMENTS**

a. DOE Order 142.1, Classified Visits Involving Foreign Nationals.

b. DOE Order 142.3, Unclassified Foreign Visits and Assignments Program.

c. Under Secretary of Energy Program Cyber Security Plan (PCSP), version 1.1.

d. 15 CFR 730-774, Bureau of Industry and Security, Department of Commerce.

7. **REFERENCES**

- a. None.

8. **DEFINITIONS**

- a. See the documents in Section 6 for needed definitions.

The most recent and official controlled hard copy version of this directive resides with NETL's Directives Coordinator. An electronic version of the controlled directive has been placed on the NETL Intranet for employee use. Printed hard copies of this electronic version are considered noncontrolled documents.

9. **REVISION HISTORY**

<b>VERSION</b>	<b>DATE</b>	<b>SUMMARY OF CHANGES</b>
Original	2/11/02	To set forth the requirements for providing access to cyber systems by foreign nationals.
A	3/8/05	Changes were made to convert the document from WordPerfect to Word.
B	10/20/08	Converted the order into the new directives format, updated the requirements documents, and added PCSP requirements.

The most recent and official controlled hard copy version of this directive resides with NETL's Directives Coordinator. An electronic version of the controlled directive has been placed on the NETL Intranet for employee use. Printed hard copies of this electronic version are considered noncontrolled documents.