DEPARTMENT OF THE INTERIOR
BUREAU OF OCEAN ENERGY MANAGEMENT, REGULATION AND ENFORCEMENT MANUAL

TRANSMITTAL SHEET

Release No. 335

SUBJECT: Administrative Series
Part 444: Physical Protection and Building Security
Chapter 3: Access Control Policy

EXPLANATION OF MATERIAL TRANSMITTED:

This manual chapter sets forth the policies for that part of the Bureau of Ocean Energy Management, Regulation and Enforcement's (BOEMRE) security program designed to safeguard BOEMRE personnel and facilities.

Walter D. Cruickshank
Acting Director

FILING INSTRUCTIONS:

REMOVE:				INSERT:			
Part	Chapter	Pages	Release	Part	Chapter	Pages	Release
				444	3	4	335

OPR: Chief of Staff Office, Administration and Budget
Date: FEB 15 2011

Bureau of Ocean Energy Management, Regulation and Enforcement
Bureau of Ocean Energy Management, Regulation and Enforcement Manual

Effective Date:
Series: Administrative
Chapter 3: Part 444: Physical Protection and Building Security, Bureau of Ocean Energy Management, Regulation and Enforcement (BOEMRE) Access Control Policy

Originating Office: Office of the Chief of Staff, Administration and Budget (A&B)

1. **Purpose**. This chapter sets forth the policies for that part of the BOEMRE security program designed to safeguard BOEMRE personnel and facilities.

2. **Scope**. The policy established herein is applicable to all BOEMRE facilities (except the Department of Interior's Main and South Interior Buildings), whether owned or leased and to all visitors entering such property.

3. **Authority**: Departmental Manual 444, Chapter 1.

4. **Responsibilities**. For purposes of this policy, the BOEMRE officials having jurisdiction over an office, building, or other facility (hereinafter referred to as the BOEMRE official) will be the Chief of Staff, A&B, the Southern Administrative Service Center Manager, and the Western Administrative Service Center Manager. These officials may assign a designee for remote locations under their jurisdiction.

A. The BOEMRE official is responsible for safeguarding personnel and real and personal property under the control of, or assigned to, the facility. The BOEMRE official may designate a representative to perform day-to-day responsibilities for compliance with this policy.

B. The program Council of Information Management Officials (CIMO) representative shall be responsible for approving the Data Center Access Request forms in conjunction with the approved Information Technology (IT) Data Center Coordinator as outlined in Section 4.F of this policy. The program CIMO representative shall also be responsible for designating an approved program IT Data Center Coordinator for each site.

C. The Bureau Physical Security Officer is responsible for updating, maintaining, and distributing changes to the access control policy.

D. Supervisors and/or Contracting Officer Representatives (COR) are responsible for validating that a BOEMRE employee or BOEMRE contractor requires access to a facility or a special access area. These accesses are outlined in Section 6 of this policy. When required by Section 10 of this policy, the supervisor or COR will review a BOEMRE employee's/contractor's access and validate whether the access is still required.

E. Each BOEMRE employee/contractor is responsible for compliance with the BOEMRE access control policy to help safeguard personnel, property, and data at facilities.

F. The approved program IT Data Center Coordinator shall be responsible for approving the Data Center Access Request form in conjunction with the Enterprise IT Representative, or their designee. The program IT Data Center Coordinator shall also be responsible for reviewing the Special Area Visitor Control Log as outlined in Section 12 of the BOEMRE Visitor Control Policy. Program IT Data Center Coordinators for each location shall be designated in writing by their respective program area CIMO representative. The Enterprise IT Representative shall be the Enterprise Support Contract COR or their designee.

G. The BOEMRE official at each location shall designate an individual or individuals who shall be identified as access control system administrators. These administrators shall be responsible for receiving the approved Data Center Access Request forms and granting the actual access. This individual or individuals will be responsible for providing quarterly reports to the program IT Data Center Coordinator and the BOEMRE official, or their designee; removing access to facilities and Data Center areas; and disabling and enabling access when temporary access has been granted as outlined in Section 5 of this policy. These reports shall contain the name of the individual having access to the data center, the date access was granted, the date access is due to expire, and the date the individual last accessed the data center.

5. **Access**. For purposes of this policy, BOEMRE shall recognize four types of access.

A. General Access. General access is defined as common areas where all Federal employees/contractors have a need to access on a day-to-day basis. These general access areas include, but are not limited to, entrances to buildings, work areas, and public access areas. This access is automatically granted to all Federal employees/contractors who have been authorized to receive a Federal identification badge as outlined in Homeland Security Presidential Directive 12 and Federal Information Processing Standards 201. This access is typically valid during normal operating hours from 6:00 a.m. to 6:00 p.m.

B. Data Center /Special Access Areas. Access to Data Centers, i.e., computer rooms are restricted to Federal employees/contractors whose job requires access to the equipment and facilities related controls. This access is also granted to building management and local emergency personnel (fire department and law enforcement) as necessary. This type of access is defined as areas where general access as outlined in Section 5.A of this policy is not commonly authorized. Examples of special access areas are data centers, help desk areas, and telecommunications closets, etc. This type of access requires the request and approval using the Data Center Access Request Form (BOEMRE Form 081).

C. After Hours Access. This type of access is for Federal employees/contractors who have a requirement to work any hours not identified as normal working hours as outlined in Section 5.A of this policy. This type of access requires the request and approval on the Request for After Hours Access (BOEMRE Form 080) by the BOEMRE official, or their designee, at each site.

D. Temporary Access. There are two types of temporary access the BOEMRE recognizes for purposes of this policy.

(1) Lost or forgotten Federal issued identification badge. This type of access is used for BOEMRE employees/contractors who have a Federal issued identification badge but have either lost or forgotten it. Should this type of access be required, the BOEMRE employee/contractor will be required to follow the BOEMRE Visitor Control Policy prior to receiving temporary access.

(2) Visiting Federal employees/contractors. This type of temporary access is given when a Federal employee/contractor, who has been issued a Federal identification badge from another location, requires access to a facility for temporary duty purposes. This type of temporary access shall be granted by the access control system administrator who configures the visiting Federal employee's/contractor's Federal identification badge at the temporary duty location; therefore, no additional badge is required.

Any visitor or special group of visitors not identified above shall be required to call and make special arrangement prior to visiting a Bureau facility. Examples of this would be school groups, American Red Cross, health care representatives, local physical fitness gym sponsors, etc.

6. **Access Forms.** BOEMRE shall use three types of forms for granting access to any facility or special access area.

A. General Access. There is no separate access form required for gaining general access to a facility as outlined Section 5.A of this policy. When a BOEMRE employee/contractor has completed the requirements for obtaining an identification credential, they will be granted general access to a facility.

B. After Hours Request Form (BOEMRE Form 080). This form is used when a Federal employee/contractor requires access to any BOEMRE facility outside normal operating hours.

C. BOEMRE Data Center Access Request Form (BOEMRE Form 081). This will be used to request, justify, and approve/disapprove access to any BOEMRE data centers or special access areas as outlined in Section 5.B of this policy.

7. **Exceptions.** Each BOEMRE facility has personnel that require access to facilities and special access areas due to the unique nature of their responsibilities. Examples of these types of personnel are facilities specialists, building security staff, building owners, building engineers, certain law enforcement officials, and emergency personnel. These types of excepted personnel are granted access based on their needs. Each BOEMRE official, or their designee, shall identify these exceptions and maintain, monitor, and update a list of them as outlined in Section 10.C of this policy.

8. **Data Center Visitor Control Logs.** In locations where BOEMRE has a data center where network equipment is located, a data center visitor control log shall be established to monitor visitors requiring non recurring access to the data center. This data center visitor control log shall be in compliance with Section 9 of the BOEMRE Visitor Control Policy. This log shall be located inside the data center, or other special access area, just inside the access point.

9. **Escorting of Data Center Visitors.** For purposes of this section, visitors are defined as anyone who has not been granted unlimited access to the data center. All visitors to any data center shall be escorted by a BOEMRE employee/contractor who has unlimited access to these areas. Visitors are prohibited from being unescorted, at any time, during their visit.

10. **Periodic Review of Access.**

A. General access. There shall be no periodic review for this type of access. The current exit clearance process will satisfy review process for purposes of this policy.

B. After hours access. The approval form (BOEMRE Form 080) requires expiration dates be specified and the access control administrator shall be required to set access according to the expiration dates identified on BOEMRE Form 080. The access control administrator shall submit a report to BOEMRE official for their review by January 10, of each year.

C. Data Center/Special Access Areas. The designated access control system administrator at each location shall submit a monthly access report to the program IT Data Center Coordinator by the 10th day of each month. This report shall clearly indicate the BOEMRE employees/contractors currently having access to the special area. The program IT Data Center Coordinator shall inform the access control system administrator and the BOEMRE official of any required changes. Additionally, the access control administrators shall submit their reports to the BOEMRE officials on an annual basis, by January 10 of each year.

11. **Compliance of Policy.** Failure to comply with this policy will be immediately reported and could result in disciplinary actions. Repeated noncompliance to this policy will be elevated to the applicable Associate Director.