

Lewis Sumner  
Vice President  
Hatch Project Support

Southern Nuclear  
Operating Company, Inc.  
40 Inverness Parkway  
Post Office Box 1295  
Birmingham, Alabama 35201  
Tel 205.992.7279  
Fax 205.992.0341



July 2, 1997

Docket Nos. 50-321  
50-366

HL-5412

U. S. Nuclear Regulatory Commission  
ATTN.: Document Control Desk  
Washington, DC 20555

Edwin I. Hatch Nuclear Plant  
10 CFR 73.55(d)(5) Exemption Request  
Use of Biometric Screening in Protected Area Access Control

Gentlemen:

In accordance with the provisions of 10 CFR 73.5, "Specific Exemptions," Southern Nuclear Operating Company (SNC) hereby requests an exemption from a requirement in 10 CFR 73, "Physical Protection of Plants and Materials." The enclosed request is for exemption from the requirement in 10 CFR 73.55(d)(5) that an individual not employed by the licensee (SNC), who requires frequent and extended access to protected and vital areas (i.e., a contractor), be authorized access to protected and vital areas without escort if the individual receives a picture badge upon entrance into such areas and returns the picture badge upon exit from such areas (i.e., not allowed to take the picture badge off-site).

This requested exemption is to allow the use of a biometric access control system which will incorporate hand geometry to control unescorted access into the site protected area (PA) of the E. I. Hatch Nuclear Plant (HNP) and which will eliminate the need to issue, store, and retrieve identification badges from a central location on site. The enclosure provides a description of the relevant aspects of the current and proposed systems, and provides the basis for this exemption request. Exemptions from this specific requirement in 10 CFR 73.55(d)(5) have been previously approved by the Nuclear Regulatory Commission (NRC) for SNC, Georgia Power Company, Florida Power and Light Company, Arizona Public Service Company, Virginia Electric and Power Company, Baltimore Gas and Electric Company, and Tennessee Valley Authority.

After issuance of the requested exemption and implementation of the biometric access control system at HNP, SNC will revise the Hatch Physical Security Plan (PSP) and provide the changes to the NRC in accordance with 10 CFR 50.54(p). SNC requests NRC approval of this exemption by December 31, 1997, in order to facilitate implementation of the biometric access control system during the early 1998 timeframe.

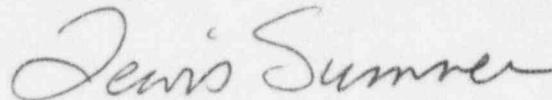
5003/1

9707150300 970702  
PDR ADOCK 05000321  
F PDR



If there are any questions or if additional information is needed, please contact this office.

Sincerely,



H. L. Sumner, Jr.

SMS/ld

Enclosure: 10 CFR 73.55(d)(5) Rule Exemption Request

cc: Southern Nuclear Operating Company  
P. H. Wells, Nuclear Plant General Manager  
NORMS

U. S. Nuclear Regulatory Commission, Washington, D. C.  
Mr. N. B. Le, Licensing Project Manager

U. S. Nuclear Regulatory Commission, Region II  
Mr. L. A. Reyes, Regional Administrator  
Mr. B. L. Holbrook, Senior Resident Inspector

## Enclosure

### E. I. Hatch Nuclear Plant Exemption Request From A Requirement of 10 CFR 73.55(d)(5)

#### Introduction

Southern Nuclear Operating Company (SNC) requests, in accordance with the provisions of 10 CFR 73.5, "Specific Exemptions," an exemption from certain requirements of 10 CFR 73.55, "Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors Against Radiological Sabotage," for the E. I. Hatch Nuclear Plant (HNP). Specifically, SNC requests an exemption from the requirement in 10 CFR 73.55(d), "Access Requirements," section (5), which requires in part: "An individual not employed by the licensee but who requires frequent and extended access to protected and vital areas may be authorized access to such areas without escort provided that he receives a picture badge upon entrance into the protected area which must be returned upon exit from the protected area.... "

10 CFR 73.55(a), "General Performance Objective and Requirements," states in part: "The licensee shall establish and maintain an on-site physical protection system and security organization which will have as its objective to provide high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety." Additionally, it states in part: "The Commission may authorize an applicant or licensee to provide measures for protection against radiological sabotage other than those required by this section if the applicant or licensee demonstrates that the measures have the same high assurance objective as specified in this paragraph and that the overall level of system performance provides protection against radiological sabotage equivalent to that which would be provided by paragraphs (b) through (h) of this section and meets the general performance requirements of this section."

This exemption request is to allow contract personnel to take their picture badge off-site in conjunction with the use of a biometric system incorporating hand geometry for the control of unescorted access into the protected area of HNP.

#### Current Manual Access Control System

Unescorted access into the HNP protected area is currently controlled through the use of a cardkey picture badge and associated personal identification number (PIN). Upon successfully passing through explosive and metal detection devices and having personal items screened by an x-ray machine, an individual attempting to gain access into the site protected area (PA) must first request a personal cardkey picture badge from Security Department personnel located in the Plant Entry and Security Building (PESB) badge island using a unique identifier. The responding officer then uses the photograph on the picture badge to verify the identity of the individual requesting access. Upon successful verification, the officer then issues the cardkey picture badge to the individual through an opening in the PESB badge island.

## Enclosure

### Exemption Request From a Requirement of 10 CFR 73.55(d)(5)

Once an individual receives the cardkey picture badge from the Security Department officer located in the PESB badge island, the individual then proceeds to the turnstile area, activates the cardkey by swiping it through a card reader mounted in front of a turnstile, and enters a PIN on the corresponding card reader keypad. Upon receiving verification by the security computer that the code entered matches the cardkey read, a permissive is supplied by the security computer to unlock the PA entry turnstile and the individual is notified of a successful operation by means of a green light and a display message, "ACCESS GRANTED," on the card reader. Once entry to the PA has been obtained, access to site vital areas (VAs) is attained by utilizing a similar automated access control system, the one exception being that a PIN number is not required.

Upon exit from the PA, the individual is required to swipe the cardkey picture badge through a card reader in order to de-activate the cardkey in the security system computer. The individual is notified of a successful swipe by means of a green light on the card reader and then deposits the cardkey picture badge into an opening in the PESB badge island. Subsequently, a Security Department officer retrieves the cardkey picture badge and places it in a designated location in the PESB badge island for storage. Therefore, under the current system, cardkey picture badges for all individuals are issued, activated, de-activated, and stored at the PESB. Under this system, the badges used to grant access to the PA are not taken off-site by either SNC or contract personnel.

#### Proposed Biometric Access Control System

Each individual who is authorized unescorted access will have the physical characteristics of one hand assigned to a unique cardkey picture badge in the security computer database. Access to the PA will be controlled in the following manner. An individual requesting PA access will swipe the cardkey picture badge through a card reader located at an entrance turnstile and, when prompted, place the appropriate hand into the biometric hand geometry reader. If the characteristics of the hand geometry being read equal or exceed a pre-defined score in the security computer assigned to the cardkey previously presented, access will be granted and the entry turnstile unlocked. The individual will be notified of a successful attempt by means of a display message, "ID VERIFIED," on the hand geometry reader. If the hand geometry characteristics do not equal or exceed the pre-defined score of the stored geometry, access will be denied by the security computer. An individual will be notified of an unsuccessful attempt by means of a display message, "TRY AGAIN," on the hand geometry reader. In addition, Security personnel in both the central alarm station and secondary alarm station (CAS/SAS) will be notified by means of an alarm message on the respective security computer terminals.

Upon exit from the protected area, the individual will swipe the cardkey picture badge through an exit card reader which will record the exit in the security computer and de-activate the cardkey. The individual will then retain the cardkey picture badge in anticipation of the next entry into the PA. Should an individual fail to swipe the cardkey upon exit, the security computer will not allow subsequent re-entry into the PA without Security personnel intervention. Since the card reader at the PA exit will suffice to record egress from the PA in the security computer, no hand geometry readers will be located at the PA exit. As a cardkey picture badge alone will not provide an individual access into the PA without the corresponding hand geometry, there will no longer be a

## Enclosure

### Exemption Request From a Requirement of 10 CFR 73.55(d)(5)

need for the on-site storage of badges and the associated distribution system. Therefore, it is intended that all personnel with unescorted access privileges, including contractors, be allowed to take their cardkey picture badges off-site. In the event that a cardkey picture badge is lost or stolen while off-site, it would be of no benefit to a potential intruder as they would be unable to defeat the biometric screening by the hand geometry reader which is necessary for PA access.

Visitors to the PA will not use the biometric access control system but will be granted access in a manner consistent with existing procedures which requires them to remain under the control and surveillance of an escort granted unescorted authorized access. There will be no change in the method of processing, controlling or escorting visitors within the PA or VA as a result of the implementation of the biometric access control system.

The issuance, storage, and retrieval of cardkey picture badges and the use of personal identification numbers will be the only access control processes eliminated upon conversion from the current access control process to a system incorporating biometric screening. All other access control processes will remain the same (e.g., search function capability, explosive detection, and metal detection). The security person responsible for the last access control function shall continue to be isolated within a bullet-resisting structure in order to assure the individual's ability to respond or to summon assistance. A uniquely identified cardkey picture badge will continue to be issued to all individuals who are authorized unescorted access to PA. The continuous display of these picture badges by all individuals inside the PA shall continue to be required. Under these circumstances, the use of an access control system incorporating biometric screening will maintain the same high level of assurance that access is granted only to authorized individuals.

#### Biometric Access Control System Features

The biometric access control system provides a non-transferable means of identifying that the individual possessing a cardkey picture badge is the individual who is granted unescorted access. Sandia National Laboratories conducted testing which demonstrated that the hand geometry equipment possesses strong performance characteristics. Specifically, this testing demonstrated that the system can meet a detection probability of 90 percent with a 95 percent confidence level. Details of the testing performed are in the Sandia report, "A Performance Evaluation of Biometric Identification Devices," SAND91-0276•UC-906, Unlimited Release, June 1991. A process for testing the system in accordance with vendor guidelines will be developed to ensure continued performance of the system to meet the general performance requirements of 10 CFR 73.55(d)(5).

#### Basis For Exemption

As discussed above, implementation of the biometric access control system at HNP is an acceptable alternative measure for protection against radiological sabotage that meets the same high assurance objective and the general performance requirements of the regulation. Also, the overall level of the biometric access control system performance provides protection against radiological sabotage equivalent to that which is currently being used. In fact, since a unique cardkey picture badge and matching non-transferable hand geometry will both be necessary for

Enclosure

Exemption Request From a Requirement of 10 CFR 73.55(d)(5)

access into the site protected area under the planned biometric access control system, the level of access control at HNP will actually be improved over the current system which utilizes a cardkey picture badge and associated personal identification number.

#### Conclusion

In conclusion, SNC has determined that implementing the biometric access control system at HNP is authorized by law and will not endanger or unduly compromise personnel safety, plant property, and/or plant security. Therefore, SNC requests that the NRC grant an exemption from the requirement in 10 CFR 73.55(d)(5) which requires that individuals not employed by SNC (i.e., contractors), who are authorized unescorted access into the protected area, return their picture badges upon exit from the protected area.