10 CFR 73.22(f)(3)

APS *A subsidiary of Pinnacle West Capital Corporation*

Palo Verde Nuclear
Generating Station

Dwight C. Mims
Sr. Vice President
Nuclear Regulatory and Oversight

Tel. 623-393-5403
Fax 623-393-6077

Mail Station 7605
P. O. Box 52034
Phoenix, Arizona 85072-2034

102-06487-DCM/DLK
March 9, 2012

ATTN: Document Control Desk
U.S. Nuclear Regulatory Commission
Information Security Branch
Washington, DC 20555-0001

References: (1) Title 10, Code of Federal Regulations Part 73.22(f)(3)
(2) National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP)

Dear Sirs:

Subject: **Palo Verde Nuclear Generating Station (PVNGS)**
Units 1, 2, and 3
Docket Nos. STN 50-528, 50-529, and 50-530
Request for Approval of Secure Voice Communications
CCORE Module by Cellcrypt Limited

Per 10 CFR 73.22(f)(3) (Ref. 1), Arizona Public Service Company requests approval to use mobile telephone devices to transmit safeguards information with the Cellcrypt Mobile^{TM} application and the CCORE Cryptographic Module by Cellcrypt Limited. This module meets the requirements of Federal Information Processing Standard (FIPS) 140-2 per the latest validation list of Reference 2. Enclosed is Validation Certificate No. 1310 for the CCORE Cryptographic Module.

If you have any questions, please contact Thomas Weber, nuclear regulatory affairs department leader, at (623) 393-5764.

S001A
NRR

Arizona Public Service Company makes no commitments in this letter.

Sincerely,

FOR D.C. MIMS

DCM/TNW/DLK

Enclosure: FIPS 140-2 Validation Certificate No. 1310 for CCORE Module by Cellcrypt Limited

cc:	E. E. Collins Jr.	NRC Region IV Regional Administrator
	B. K. Singal	NRC NRR Project Manager for PVNGS (electronic and paper)
	L. K. Gibson	NRC NRR Project Manager for PVNGS (electronic)
	J. R. Hall	NRC NRR Senior Project Manager (electronic)
	M. A. Brown	NRC Senior Resident Inspector for PVNGS

ENCLOSURE

FIPS 140-2 Validation Certificate No. 1310 for CCORE Module by Cellcrypt Limited

FIPS 140-2 Validation Certificate

The National Institute of Standards and Technology of the United States of America

The Communications Security Establishment of the Government of Canada

Certificate No. **1310**

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the Cryptographic Module identified as:

CCORE Module *by* Cellcrypt Limited

in accordance with the Derived Test Requirements for FIPS 140-2, Security Requirements for Cryptographic Modules. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting *Sensitive Information* (United States) or *Protected* Information (Canada) within computer and telecommunications systems (including voice systems).

Products which use the above identified cryptographic module may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life cycle, continues to use the validated version of the cryptographic module as specified in this certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

This certificate includes details on the scope of conformance and validation authority signatures on the reverse.

TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S., or Canadian Governments.

FIPS 140-2 provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range and potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of a cryptographic module. The scope of conformance achieved by the cryptographic modules as tested in the product identified as:

CCORE Module *by* Cellcrypt Limited
(Software Version: 0.6.0-rc3; Software)

and tested by the Cryptographic Module Testing accredited laboratory: ***CEAL: a CygnaCom Solutions Laboratory, NVLAP Lab Code 200002-0***
CRYPTIK Version 7.0
is as follows:

Cryptographic Module Specification:	Level 1	*Cryptographic Module Ports and Interfaces:*	Level 1
Roles, Services, and Authentication:	Level 1	*Finite State Model:*	Level 1
Physical Security: *(Multi-Chip Standalone)*	Level N/A	*Cryptographic Key Management:*	Level 1
EMI/EMC:	Level 1	*Self-Tests:*	Level 1
Design Assurance:	Level 1	*Mitigation of Other Attacks:*	Level N/A
Operational Environment:	Level 1	*tested in the following configuration(s):*	Ubuntu Server

The following FIPS approved Cryptographic Algorithms are used: **AES (Cert. #1089); RSA (Cert. #514); SHS (Cert. #1022); HMAC (Cert. #612); RNG (Cert. #611)**

The cryptographic module also contains the following non-FIPS approved algorithms: **RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength); RC4; MD5; EC Diffie-Hellman (non-compliant); ECDSA (non-compliant)**

Overall Level Achieved: 1

Signed on behalf of the Government of the United States

Signature: Donna F. Dodson

Dated: May 19, 2010

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: May 10, 2010

Director, Industry Program Group
Communications Security Establishment Canada