(U) As weapon and control hardware evolve, improvements and changes are expected to occur. Because a mix of old and new systems is likely to remain, it may not be possible to utilize some capabilities fully. Study of goals and requirements is warranted to give direction to acquisition of future systems.

4. PAL Advanced Development (U)

(U) Today's PAL hardware elements and code management system were described in Section 2. New concepts in both hardware and code management are now in various stages of development. These concepts are summarized in this section.

4.1 New PAL Weapon Systems (U)

(U) The W84 warhead for the GLCM, which is scheduled for deployment in late 1983, is the most recent PAL weapon system described in Section 2. Several other new systems are in various stages of development or production.

DOE
b(3)

(U) The W79 8-in. AFAP preceded the W84, entering Phase 6 production in September 1981. Ultimately the W79 will replace the W33 8-in. projectile in stockpile. However, a date for overseas deployment is uncertain at this time. The W79 is equipped with the MC2907 MCCS that provides CAT D PAL protection.

(C) The W85 PII warhead begins Phase 6 production in May 1983. Eventually, the improved PII system will replace many PIs presently deployed to NATO. The W85 is basically a B61-4, CAT F warhead adapted to the warhead section of the PII missile. As such, it is equipped with an MC2907A MCCS.

(C) The W82 155-mm AFAP that will replace the W48 projectile is presently scheduled to enter Phase 6 production in June 1986. No deployment date has been announced. The W82 will be equipped with the MC3764 CAP (Section 4.2). The CAP will provide the same multiple code population and limited-try features as the MCCS, but the W82 will not be maintained in a disenabled state by interrupting warhead circuitry. Instead, the CAP will be located outside the weapon in a Use Denial Lock (UDL). The UDL (Figure 44) is a device which fastens to the nose of the projectile, preventing installation of the fuze. Unlocking the CAP allows removal of the UDL. An Integrated Control Unit (ICU) in the shipping container of each round will provide unlock and relock control of the UDL (Figure 45).

(U) A factory-rebuild program is currently under way to upgrade early versions of the B61. The B61-6 will result from retrofitting the B61-0 with enhanced safety features and the MC2907 CAT D PAL. First Phase 6 production is scheduled for October 1985. The B61-8 represents a safety upgrade of the B61-2 and B61-5. The B61-8 will have an MC2907 CAT D PAL and is scheduled for initial Phase 6 production in January 1988.

(U) Four strategic systems with PAL are planned for the stockpile. Two of these are modifications of existing systems. The B28 (Mods 0 and 1) will be field retrofitted (beginning April 1983); B61-1 will be factory rebuilt (Phase 6 begins September 1985) into the B61-7. Present plans call for an MC2907 CAT D PAL in both systems. Two new strategic systems, the W80-1 warhead for the Air-Launched Cruise Missile (ALCM) (Phase 6 production began February 1982) and the B83 modern strategic bomb (Phase 6 production is scheduled to begin September 1983), also will be equipped with the MC2907 CAT D PAL.

(U) Two new PAL-equipped Navy systems are currently planned. Both the W80-0 warhead for the Tomahawk Sea-Launched Cruise Missile (SLCM) (Phase 6 production is to begin April 1984) and the W81 warhead for the SM-2 fleet air defense missile (Phase 6 production to begin November 1986) will have CAT D PAL (MC2907 or MC3764).

(U) A stockpile projection[31] (Figure 46) shows the planned distribution of PAL-equipped weapons (weapons with no PAL are not shown) through FY 1992. This projection reflects the planned production of weapons equipped with modern CAT D and F PAL devices.

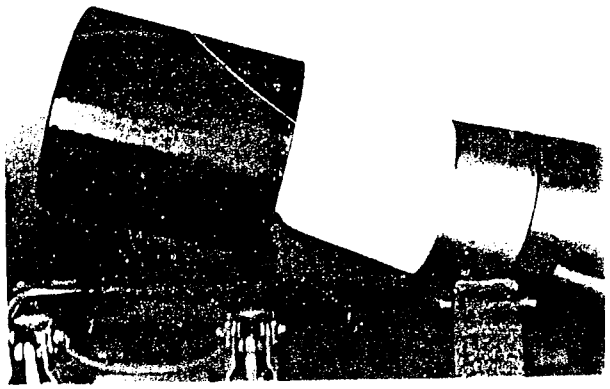

Figure 44. Use Denial Lock (U)

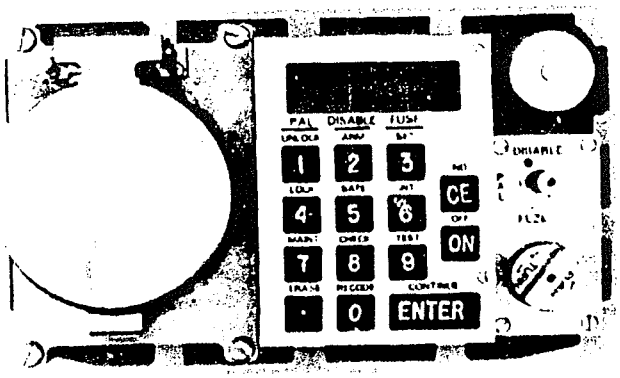

Figure 45. Integrated Control Unit (U)

- Encrypted recode—the ability to recode using encrypted data, thus lessening concerns about bugging and emanation
- Encrypted code check

(U) New operations that are not under code control include:

- Recovery of weapon ID
- Self test

(U) Current control equipment does not allow the operator to take full advantage of these additional features. Software modifications could make the APC compatible with the additional recode capabilities of the CAP.

(U) In addition to new functions, the CAP will have a higher tolerance for voltage fluctuations in the input signals than does the MCCS and will withstand harsher shock and radiation environments. Finally, the CAP will have a more flexible output structure that can be tailored to the needs of the weapon designer.

4.2 The Code Activated Processor (U)

(U) The Code Activated Processor (CAP) is the next generation PAL device. It is being developed as a replacement for the MCCS, which will become increasingly difficult to manufacture because of decreasing component availability and obsolete technology.

(U) The microprocessor-based CAP is being designed as a drop-in replacement for the MC2907; it will have the same size and weight and will emulate the MCCS input and output signals. It will be compatible with all existing CAT D and F control equipment and will have limited-try and code population features identical to those of the MCCS.

(U) The CAP will also have a number of capabilities beyond those provided by the MCCS. First, several additional operations will be possible. Some of those operations will be under code control. These include:

- Maintenance lock—a UDL requirement
- Recovery of recode status information
- Storage and recovery of weapon state-of-health data

4.3 Asymmetric Crypto PAL (U)

(U) The Asymmetric Crypto PAL (ACP) is an advanced PAL that has been under exploratory development.[32] It consists of an electronic coded-switch system whose inputs are processed by an asymmetric cryptographic system.

(U) Like the CAP, the ACP could provide recode and verification operations which are encrypted communications with the PAL controller. This reduces the vulnerability of the system to bugging and emanation. The asymmetric nature of the ACP crypto system also provides protection against code extraction, e.g., the determination of a code/combination by dissection or probing of a PAL to read its memory.

(U) The ACP has reached a stage of development marked by the completion of demonstration hardware. Although the system is feasible, development timescales for operational hardware depend on the availability of special large-scale integrated circuits that are needed for implementation of the cryptographic system.

4.4 Headquarters Equipment for Peacetime Code Management (U)

(U) The T1565 Headquarters Code Processor (HCP) is being developed in parallel with the T1563 APC as a peacetime code management aid. While the APC can (and will, initially) function by itself, the HCP will provide a number of additional capabilities.

(U) The HCP (Figure 47) is built around an HP 1000 computer. The system includes a printer, CRT display screen, keyboard, tape and disc storage units, and a cryptographic system. HCP operation is depicted in Figure 48. It has a number of functions. First, it provides access, under two-man control, to encrypted code information from the source data module generated by NSA. In addition, it contains a weapon data base that may be periodically updated. This data base would include, for example, the theater weapon inventory information: mark and mod, serial number, and location of weapons in theater. Utility programs will be available for correlating the data base information with the weapon code information to aid in the construction of theater code plans. Given a theater code plan, the HCP will be able to generate the appropriate portable data modules for use by APCs during recode operations. The HCP will also be capable of reading monitor modules generated by the APC during recode. This may eliminate the need for on-site recode verification by the PMCT in cases where recode can be done with the APC.

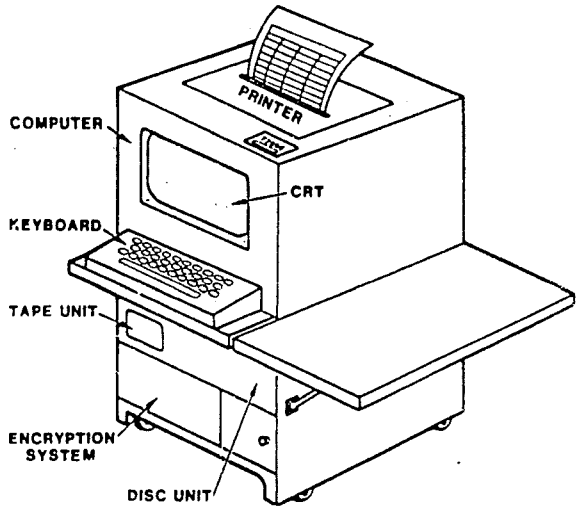

Figure 47. T1565 HQ Code Processor (U)

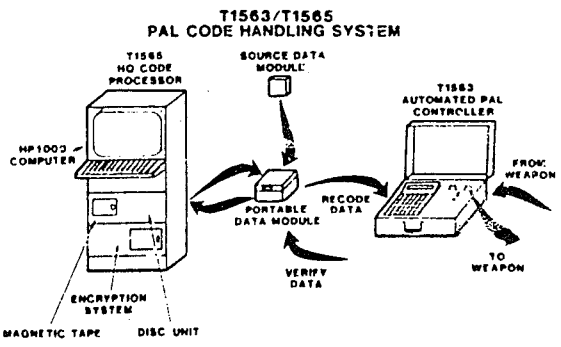

Figure 48. T1563/T1565 PAL Code Handling System (U)

DOE
b(3)

DOE
4(3)

DOE
b(3)

DoE
b(3)

These differences include:

- A PAL inventory made up almost entirely of Modern PAL devices featuring limited-try, multiple code capability, and code populations $\geq 10^6$
- A significant fraction of the deployed stockpile equipped with APSs
- An APC that will permit "no knowledge" recode operations and remote verification

(U) In the long term, these efforts address the preponderance in today's stockpile of Old PAL devices and the resource limitation of the theater code management organizations.

(U) Identification of needed system improvements presupposes the ability to compare the function of the existing system with a set of performance criteria to determine system deficiencies. Today, performance criteria for PAL, based on an analysis of the overall command and control systems of which PAL is but one element, do not exist. In addition, it is not possible to estimate or measure the performance of PAL without a useful threat definition. No such definition is presently available. Thus it has not been possible, within the context of this report, to determine what improvements are needed in today's PAL system. Definitions of the purpose of PAL, in terms of a useful definition of threat(s) and of the role of PAL within the command and control structure, are needed to evaluate the performance of today's systems and the utility of new technology. Given a useful specification of the purpose and role of PAL for TNWs, a number of other issues could be explored.

DOE
b(3)

Intentionally Left Blank

References (U)

[1]*European Theater Nuclear Weapons Command, Control, and Communications (TNWC³) System Improvement Plan (SIP)* (U), Draft Report (Washington, DC: Defense Communications Agency, 15 December 1980). SFRD.

[2]*Pacific Theater Nuclear Forces Command, Control, and Communications (PACOM TNFC³) System Improvement Plan (SIP)* (U), Draft Report (Washington, DC: Defense Communications Agency, 22 January 1982). SFRD.

[3]*Joint Army/ERDA Evaluation of Command, Control, and Security of Army Nuclear Weapon Systems*, 01794-77-00 (Washington, DC: Army/Energy Research and Development Administration, 16 May 1977). Secret.

[4]*Nuclear Weapon Security Manual* (U), DOD5210.41-M, Change (Washington, DC: Department of Defense, 1 September 1978). Confidential.

[5]*Policy and Procedures Governing the Permissive Action Link/Coded Switch/Positive Enable Cipher System* (U), JCS Pub 13, Vol II (Washington, DC: JCS, 1 January 1981, Rev 9 June 1981). SFRD. Hereafter cited as JCS Pub 13.

[6]"Permissive Links for Nuclear Weapons in NATO," memo from President J. F. Kennedy to Secy of State, Secy of Defense, Chairman of AEC, Dir Bur of Budget, NSAM-160, RS3446/53567, 6 June 1962. Secret.

[7]R. S. Pinkham, W. L. Clement, and A. M. Jackson, *Characteristics and Development Report for the MC1707 Coded Switch* (U), SC-DR-65-62, November 1965. Confidential.

[8]D. P. Roberts and J. H. Barnette, *Characteristics and Development Report for the MC1707A Coded Switch* (U), SC-DR-67-833, December 1967. Confidential.

[9]S. V. Asselin, *Countersink Program Final Report*, RS1514/643, September 1969. Secret.

[10]*Final Development Report on the W70 Warhead* (U), SLL73-0035, February 1974. Secret.

[11]R. E. Bair et al, *MC2764 Multiple Code Coded Switch Development Report* (U), SAND74-0228 (Albuquerque, NM: Sandia Laboratories, December 1974). Confidential

[12]M. M. Newsome and P. H. Stokes, *The Multiple Code Coded Switch*, SC-DR-66-422, August 1966.

[13]*Preliminary Development Report for the MC2707 Security Container System Used With the XM517 AFAP*, RS3410/2027, SC-WD-70-508, January 1971. CFRD.

[14]*Preliminary Development Report for the W75/XM673 Category E PAL* (U), RS3150/2410, SLA-73-0061, October 1974.

[15]"Phase 3 Authorization for B57 and B61 With Integral Protective System (IPS)," letter from Maj Gen E. B. Giller, OMA, to J. A. Hornbeck, 18 April 1972.

[16]*Nuclear Weapon System Safety Design and Evaluation Criteria*, AF Regulation 122-10, 7 November 1975.

[17]Atomic Energy Act of 1954, PL 703, Section 92.

[18]*General Characteristics for Permissive Devices for Use With Nuclear Weapons*, RS4323/1036, 13 September 1962. SFRD.

[19]*General Characteristics for Permissive Action Link Systems for Use With Nuclear Weapons*, RS4324/1035, 27 October 1969. SFRD.

[20]*General Characteristics for Permissive Action Link Systems for Use With Nuclear Weapons*, RS3148-1/95912, 26 July 1972. SFRD.

[21]*General Characteristics for Permissive Action Link System for Use With Nuclear Weapons*, RS2612/80/0302, 18 April 1980. SFRD.

[22]JCS Pub 13, op cit.

[23]*USCINCEUR Operational Concept for Theater Nuclear Forces Comand, Control, and Communications System (TNFC3S)*. (U) (Washington, DC: Defense Communications Agency, 16 April 1980), p II-6. SFRD. Hereafter cited as USCINCEUR.

[24]*CINCPAC Operational Concept and Required Operational Capabilities for Theater Nuclear Forces Command, Control, and Communications System (TNFC3S)* (U), Vol I (Washington, DC: Defense Communications Agency, 27 July 1981). SFRD. Hereafter cited as CINCPAC.

[25]*Nuclear Weapon Security Manual*, op cit.

[26]Policy and Procedures Governing the Permissive Action Link/Coded Switch/Positive Enable Cipher System, 1 January 1980, JCS Pub 13, Vol II.

[27]Letter from J. P. Wade, Chairman, Military Liaison Committee, to D. C. Sewell, Assistant to Secretary of Defense for Planning, 18 April 1980.

[28]*Measures for Upgrading Nuclear Weapons Safety and Security*, (U), OATSDAE, USDRE 83-0275, February 1983.

[29]CINCPAC, op cit.

[30]USCINCEUR, op cit.

[31]*Nuclear Weapons Production and Planning Directive (P&PD) 80-0* (U), Military Application (Washington, DC: Department of Energy, 31 March 1980). SRD.

[32]T. S. Edrington, *Asymmetric Crypto PAL* (U), SAND82-1665 (Albuquerque, NM: Sandia National Laboratories, December 1982). SFRD.

Intentionally Left Blank