ASSISTANT SECRETARY OF DEFENSE

6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

COMMAND, CONTROL
COMMUNICATIONS
AND INTELLIGENCE

August 5, 2002

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Guidance and Provisions for Developing Department of Defense (DoD) Component's Public Key Enabling (PKE) Policy Compliance Waiver Process

On May 17, 2001, the DoD Chief Information Officer (CIO) issued policy for PKE of DoD applications in the memorandum "Public Key Enabling of Applications, Web Servers, and Networks for the Department of Defense." The policy provides specific guidelines for PKE networks, web servers, and client software applications, and assigns responsibility to the Defense-wide Information Assurance Program (DIAP) for policy compliance oversight to include publishing guidance and provisions to Component CIOs in the development of waiver processes.

The policy further authorizes DoD Component CIOs to waive compliance to PKE policy for individual applications on a case-by-case basis consistent with the waiver guidelines and provisions published by the DIAP (attached). Component CIOs may only grant waivers for the minimum length of time required for achieving compliance. In addition, the policy requires that any PKE compliance waiver shall be reported to the DIAP within 15 days of approval by the Component CIO. The following are prospective reasons for CIOs to consider granting PKE compliance waivers:

1. Legacy systems to be replaced in the near term with a PK-Enabled system,

2. Anticipated costs of PK-Enabling that are deemed unreasonable, or
3. Other undue hardships.

Compliance with the October 2003 milestones in the Public Key Infrastructure Policy Update memorandum dated May 21, 2002 is expected, and waivers should only be considered for exceptional cases. It is strongly recommended that the DoD Component CIO develop and publish a component-specific waiver process consistent with the DIAP waiver guidelines, if the CIO anticipates processing more than a few waivers.

My point of contact for the guidance and provisions for the development of component PKE compliance waiver processes is Mr. Eustace King, ODASD (S&IO)/IA/DIAP, telephone 703-602-9969, email: eustace.king@osd.mil.

John P Stenbit

John P. Stenbit

Attachment

1. WAIVER PROCESS DEVELOPMENT

Each DoD component CIO has the authority to waive compliance to the PKE policy. If a Component CIO anticipates processing more than a few waivers, it is strongly recommended that a component-specific waiver process be developed and published. To assist the component CIOs in their efforts to develop their waiver processes, the DIAP, as mandated by the PKE policy, is providing the guidance for developing a process and defining procedures in this attachment.

Component's Public Key Enabling Policy Compliance Waiver Process

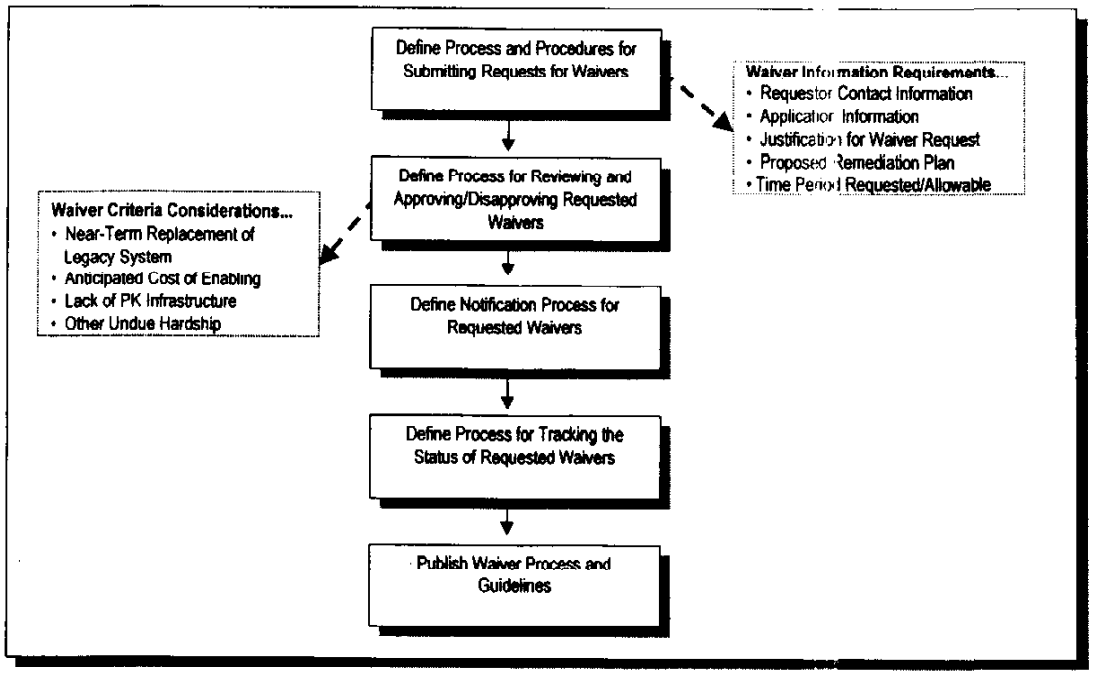

Figure 1

1.1 Define Process and Procedures for Submitting Requests Waivers. All waiver requests should be submitted in writing and signed by the application manager. The application manager is defined for purposes of this document as the individual with primary responsibility for operation and oversight of a particular application. The application manager should balance the need for compliance with the stated requirements and goals of the DoD PKE policy, with other factors such as interoperability, scheduled near term application replacement, anticipated enabling costs, and availability of existing PKI architecture. Where the application manager determines that a waiver may be appropriate, a written request for a policy compliance waiver should be submitted to the

component CIO. At a minimum, a waiver request should include the following information:

- Requestor contact information
- Application information for which a waiver is being requested (see figure 1)
- Section(s) of the PKE policy for which a waiver is being requested
- Justification for the waiver request (see section 1.2.1 below)
- Description/justification for requested waiver
- Proposed remediation/mediation plans including actions, resources and milestones
- Time period for which waiver is being requested, in compliance with maximum allowable periods as determined by the component CIO

1.2 Define Process for Reviewing Requested Waivers. The component CIO should review the contents of the waiver package and determine whether or not to approve the waiver request based on the merits of the request and the requirements of the PKI and PKE policy. While the decision to approve or disapprove a waiver request is at the discretion of the DoD component CIO, the following criteria, which are consistent with the PKI and PKE policies, should be considered in the decision-making process.

1.2.1 Waiver Criteria.

- Legacy System to be Replaced Near Term with PK-Enabled System. A waiver may be appropriate where the request is for a legacy application that is covered by a current phase-out plan, and for which a public key-enabled replacement or successor application has been identified and approved, or for which approval has been requested. The waiver request must specifically identify the replacement application and demonstrate that the application will comply with the requirements of the PKE policy. In addition, the anticipated date for when the replacement application will be operable also should be included. In such cases, a waiver may be granted for a period of up to one year, or until the date on which the replacement application becomes operable, whichever is shorter.

- Anticipated Cost of Enabling. A waiver may be appropriate where the anticipated cost of enabling an application in compliance with the PKE policy is unreasonable when compared with the costs associated with enabling substantially similar applications. The waiver request must specifically detail the costs associated with enabling the application, as well as identify substantially similar applications and the costs associated with enabling those applications. It also should include an explanation of the costs and why the are expected to exceed those for similarly situated applications. In such cases, a waiver may be granted for up to one year, or until such time as an alternative solution is identified, whichever is shorter.

- Other Undue Hardship. A waiver may be appropriate in other, limited circumstances where the requestor can clearly demonstrate undue hardship that would be occasioned by complying with the requirements of the PKE policy. The mere cost of the enabling, if consistent with the costs necessary to enable other similarly situated applications, should not be sufficient to support a waiver request. In order to obtain a waiver in these circumstances, the requestor must be able to demonstrate unique circumstances requiring that the waiver be granted, and must also provide a plan for resolving the underlying issues responsible for the waiver request. In such cases, a waiver may be granted for up to six months, to allow for the resolution of the underlying issues.

1.3 Define Notification Process for Requested Waivers. If the request for a waiver is approved, the component CIO should notify the requesting application manager, in writing, that the waiver has been approved. In addition, approved waivers must be reported to the DIAP at 1215 Jefferson Davis Hwy, Suite 1101, Arlington, VA 22202-4302, within 15 days of approval. If the request for a waiver is denied, the application manager should be notified in writing and provided an explanation for the waiver denial.

1.4 Define Process for Tracking the Status of each Waiver Request. It is recommended that a process for monitoring the waiver requests be established for the purpose of tracking the status of each request and reporting component waiver request activities. The tracking process should include assigning an identifier to each request and establishing a records maintenance system for filing and archiving waiver requests. The component CIO may also consider establishing a timeframe for processing and responding to a waiver request.

1.5 Publish Waiver Process and Guidelines. Once the waiver processes have been developed and implemented, in accordance with the above guidelines, the component CIO should publish the process for access by application managers and other appropriate personnel, and provide a copy of the final policy to ASD (C3I) within 15 days of signing.