ATTENTION ALL JPAS USERS

It is a violation of DoD Regulations to share username/password, any Approved Active Public Key Infrastructure (PKI) Certificate, or allow an individual to access another person's JPAS account in any manner or form. Only the authorized account holder is permitted to access/use his/her account. Examples of Approved Active PKI Certificates are Common Access Cards (CAC) and Personal Identity Verification (PIV) cards, to include External Certificate Authority (ECA) cards.

There are no combined or "company" JPAS user accounts. Users are required to have their own Approved Active PKI Certificate and JPAS account. Individuals cannot use another person's credentials. If you are not using your own account and certificate that are assigned to you, DISCONTINUE USING JPAS IMMEDIATELY and inform your Industrial Security Representative.

Any Account Manager, authorized or unauthorized user who violates JPAS security and account management policies will risk immediate forfeiture and TERMINATION of their JPAS account, regardless of any access requirements that may exist to support mission-critical and job-essential tasks. When you select 'AGREE' at the bottom of this page, you are agreeing to comply with all JPAS administration policies, to include the forfeiture of JPAS access if terms of use are violated.

DATA YOU ARE ABOUT TO ACCESS COULD POTENTIALLY BE PROTECTED BY THE PRIVACY ACT OF 1974. You must:

• Have completed the necessary training with regards to Security Awareness and safe-guarding Personally Identifiable Information.

• Ensure that data is not posted, stored or available in any way for uncontrolled access on any media.

• Ensure that data is protected at all times as required by the Privacy Act of 1974 (5 USC 552a(I)(3)) as amended and other applicable DOD regulatory and statutory authority; data will not be shared with offshore contractors; data from the application, or any information derived from the application, shall not be published, disclosed, released, revealed, shown, sold, rented, leased or loaned to anyone outside of the performance of official duties without prior DMDC approval.

• Delete or destroy data from downloaded reports upon completion of the requirement for their use on individual projects.

• Ensure data will not be used for marketing purposes.

• Ensure distribution of data from a DMDC application is restricted to those with a need-to-know. In no case shall data be shared with persons or entities that do not provide documented proof of a need-to-know.

• Be aware that criminal penalties under section 1106(a) of the Social Security Act (42 USC 1306(a)), including possible imprisonment, may apply with respect to any disclosure of information in the application(s) that is inconsistent with the terms of application access. The user further acknowledges that criminal penalties under the Privacy Act (5 USC 552a(I)(3)) may apply if it is determined that the user has knowingly and willfully obtained access to the application(s) under false pretenses.

UNDER THE PRIVACY ACT OF 1974, YOU MUST SAFEGUARD PERSONNEL INFORMATION RETRIEVED THROUGH THIS SYSTEM.

DOD NOTICE AND CONSENT BANNER

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

- At any time, the USG may inspect and seize data stored on this IS.

- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.

- This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

Department of Defense (DOD) policy prohibits the use of web technology which collects user-identifying information such as extensive lists of previously visited sites, e-mail addresses, or other information to identify or build profiles on individual visitors to DOD publicly accessible

web sites. DOD policy, however, does permit the use of "cookies" or other web technology to collect or store non-user identifying information but only if users are advised of what information is collected or stored, why it is being done, and how it is to be used. This policy will be clarified to make clear that "persistent cookies" (i.e., those that can be used to track users over time and across different web sites) are authorized only when there is a compelling need to gather the data on the site; appropriate technical procedures have been established to safeguard the data; and the Secretary of Defense has personally approved use of the cookie.

FOUO MARKING ON ALL APPLICATION SCREENS

FOR OFFICIAL USE ONLY (FOUO)

In accordance with DoD Regulations and the Privacy Act of 1974, you must safeguard personnel information retrieved through this system. DoD Regulations are: 5 USC 301 - Departmental Regulations, DoD 5200.1-R - The Information Security Program, Title 5, United States Code, Section 552a Public Law 93-579 (Privacy Act of 1974), DoD Directive 5400.07 - The Freedom of Information Act (FOIA) Program, DoDD 5400.11-R - DoD Privacy Program, and DTM-04-009 Security Classification Marking Instructions.