

eMPN Security Plan Draft and eMPN Security Accreditation Letter
Task Order 65 – Deliverable 65.1.4
E-Sign Mad Dog

Before the eMPN system becomes operational, it must be reviewed for security vulnerabilities and risks. LO/LC completed a review which documented several security risks and the associated security controls used to mitigate those risks. Unfortunately, not all risks can be mitigated. Therefore, the system manager must accept the risks or deny permission for the system to move into full operation. For the eMPN, an interim approval to operate (IATO) was granted at the Production Readiness Review given certain conditions. For example, SFA needs to resolve the issue that areas of security responsibility have not been clearly defined among the various contractors. The risk from this responsibility issue is low to SFA, but should be addressed expeditiously.

The accreditation letter below is a draft version of the letter submitted to LO for completion prior to the Production Readiness Review. The letter is an updated version of the letter used by the Department of Education Security and Privacy Office, instructing the system manager to accept, reject, or give interim authority to operate. The final, signed version of this document will be included when it becomes available.

Additionally, a requirement for granting IATO was the addition of eMPN to the security plans for Loan Origination/Loan Consolidation. As part of the system security review performed by EDS, the contractor stated, “EDS is drafting Addenda to the current CSC Security Plan for the LC and LO websites that will include all application level controls associated with eMPN. CSC’s security plan must be taken into consideration when reviewing the addenda. Modifications will be made with regard to all significant security elements of the eMPN. The Addenda will be completed on or about June 28th, 2001.” When these addenda become available, they will be included with this deliverable.

Date:

To: Office of CIO

From: Kay Jacks, Designated Approving Authority

SUBJECT: SYSTEM SECURITY ACCREDITATION OF [SYSTEM]

A certification review of [System] has been conducted to determine its compliance with the Department's security requirements. Based on the results of the certification, and corrective actions implemented or planned to mitigate the risks associated with the identified vulnerabilities, we certify that [System] –

___ The application meets the documented and approved security requirements.

___ The application does not meet all documented and approved security requirements.

Weighing the requirements of [System] against residual risks, we recommend –

___ Full accreditation for initial/continued operation

___ Full accreditation for the initial or continued operation of the system contingent upon recommendations included in the certification evaluation report being implemented.

___ Initial accreditation for the initial or continued operation of the system contingent upon recommendations included in the certification evaluation report being implemented.

___ The application will not be accredited for initial or continued operations.

Certification of [System] at [Location] has been performed in accordance with OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," and the Department of Education Certification and Accreditation Program. The documented security requirements of [System] have been carefully reviewed and found to properly reflect controls required to protect the system and its information against unauthorized disclosure, alteration, or destruction.

A copy of this certification letter with supporting documentation generated during the certification shall be retained by the activity as a permanent record.

Signatures and Titles
