Memorandum

U.S. Department of Transportation
Office of the Secretary
of Transportation

Subject: **ACTION:** DOT Information Technology and Information Assurance Guidance Number 2009-0002: e-Authentication and Access Control

Date: May 4, 2009

Reply to:
Attn. Of:

From: Jacquelyn Patillo Jacquelyn Patillo
Acting Chief Information Officer, S-80

To: OA Chief Information Officers
OA Information System Security Officers
OA Information System Security Managers

I. Purpose

The purpose of this memorandum is to provide supplemental guidance on the implementation of electronic authentication, and access controls on U.S. Department of Transportation (DOT) IT systems, consistent with established and evolving DOT policy.

II. Scope

This guidance applies to all Information Technology (IT) Systems operated by or on behalf of DOT Operating Administrations or Departmental Offices, including systems operated by contractors, commercial entities, or other Departments/Agencies on behalf of DOT.

III. Effective Date

This guidance is effective as of the date of signature and remains in effect until canceled, amended, or replaced by subsequent guidance.

IV. References

DOT 1350.2, *Departmental Information Resource Management Manual (DIRMM), Chapter 10 – Information Assurance*, November 17, 2006
CIOP 1351.2, *Access Control (AC) Controls*, May 14, 2009
NIST SP 800-53 (rev. 3- or Latest), *Recommended Security Controls for Information Systems,* February 5, 2009
NIST SP 800-63 (rev. 2- or Latest), *Electronic Authentication Guideline,* December 12, 2008

Advancing the Use and Strategic Value of Information Technology Resources Throughout the Department of Transportation, July 29, 2008

V. Cancelations

This guidance supersedes all previous DOT guidance related to e-Authentication and implementation of access controls.

VI. Guidance

a. All DOT System Owners shall utilize NIST SP 800-60 and FIPS 199 to categorize information and information systems within their purview.

b. All DOT System Owners shall utilize the DOT e-Authentication worksheet, NIST SP 800-53, NIST SP 800-63, and the OMB e-Authentication Risk Assessment tool as appropriate to assess the risks for systems within their purview, associate those risks with an appropriate assurance level, and identify the appropriate technical controls for implementation.

   i. System Owners shall determine the appropriate level of assurance in a user's asserted identity. The potential harm or impact, and the likelihood of such impact will determine the level of risk. System Owners shall use the methodology described in OMB Memorandum M04-04 to determine the categories of harm, impact, impact values, and potential impact of authentication errors.

   ii. System Owners shall follow steps 1 through 5 articulated in OMB Memorandum M04—04 in order to determine the appropriate assurance level of each transaction requiring electronic authentication.

      1. Level 1: Little or no confidence in the asserted identity's validity.
      2. Level 2: Some confidence in the asserted identity's validity.
      3. Level 3: High confidence in the asserted identity's validity.
      4. Level 4: Very high confidence in the asserted identity's validity.

c. System Owners shall assess the level of confidence in the credential of any person asserting an identity by completing a formal assessment against the assurance level. The System Owner is responsible for identifying requirements for each step in the electronic authentication processes as described in OMB Memorandum M04-04.

d. For internally facing core transportation (mission) systems – those servicing DOT Federal and contract employees only – with assurance levels of Level 3 or Level 4, System Owners shall utilize the DOT HSPD-12 Logical Access infrastructure and DOT-issued FIPS 201 compliant PIV (personal identification verification) card to satisfy the identification and multi-factor authentication requirement for systems at these assurance levels.

    i. System Owners shall ensure that their investment exhibits, budgets, and system architectures explicitly reflect resource allocations and a roadmap to initiate integration activities for systems within their purview beginning in FY2010, as per previous guidance from the DOT Office of the Chief Information Officer.

    ii. System Owners shall not implement identity management or logical access control solutions separate from the DOT HSPD-12 logical access infrastructure without explicit written authorization from the DOT Chief Information Officer.

    iii. For systems utilizing shared infrastructure or shared platforms, OA CIOs shall ensure that the underlying shared platform authenticates to the **highest** assurance level of applications utilizing the platform. Example: A shared platform hosting internal applications with assurance levels of Level 2 and Level 4, must implement controls sufficient to satisfy Level 4 assurance requirements. The application with a Level 2 requirement may use a Level 4-compliant platform without having to satisfy the higher assurance level.

e. For externally facing systems, System Owners are responsible for implementing technologically appropriate solutions as follows:

    i. Systems with multiple e-government electronic transactions requiring multiple levels of assurance shall authenticate at the **highest** level of assurance.

    ii. System Owners shall determine the requirement for the use of anonymous credentials for transactions where there is a need to preserve anonymity. System Owners must provide written justification to the LoB/OA CIO for implementing anonymous authentication, and that justification must be registered with the system security documentation.

iii. All implementations of electronic authentication shall conform to security requirements for collecting, storing, and managing personal identifiable information (PII) as described in Section 208 of The E-Government Act of 2002.

iv. System Owners shall conduct a cost benefit analysis matching the required level of assurance against the cost and burden of business, policy, and technical requirements of the materiel solution as articulated in OMB Memorandum M04-04.

1. System Owners facing system life cycle refresh shall consider the costs and benefits of using existing e-Authentication solutions in production operation elsewhere in DOT, even when not within the owning OA.
2. System Owners preparing to design and deploy new systems with e-Authentication requirements shall utilize one of the existing solutions, unless a cost-benefit analysis shows a clear advantage to DOT – as approved by the DOT Chief Information Officer – to deploying a new e-Authentication solution.

v. In the absence of Federal e-Authentication shared service providers, System Owners and LoB/OA CIOs shall make the necessary resource commitments to implement authentication solutions to the appropriate assurance level within their system(s), and to continue to provide the requisite e-Authentication services.

All evidentiary documentation pertaining to this e-Authentication and access control guidance, as cited above, shall be available in an electronic format and shall be uploaded by an ISSO or ISSM into the DOT FISMA Reporting system (CSAM) for the corresponding OA system in order to be deemed in compliance with the associated DOT policies.

VII. Compliance

Within 30 days of the issuance of this guidance, OA CIO's shall document via signed memorandum to the DOT CIO:

- acknowledgement of this guidance and promulgation within their OA;
- acknowledgement of the FY2010 budgetary guidance for HSPD-12;
- that OA systems within their purview have been assessed for e-authentication assurance level;
- that documentation of assessment results for OA systems are captured in CSAM;
- and identify OA systems that will be targeted for initiation of development and enhancement efforts in FY2010 to integrate them into the DOT HSPD-12 Logical Access infrastructure.

Within 90 days of the issuance of this guidance, OA CIO's shall ensure that systems identified for HSPD-12 Logical Access integration have been identified via written memorandum to the DOT CIO by name and corresponding investment identifier, with cost and schedule estimates, for incorporation into the DOT HSPD-12 implementation plan.

Within 1 year from the issuance of this guidance, OA CIO's shall ensure that externally facing systems have implemented and attained the requisite e-Authentication assurance level.

Within 3 years from the issuance of this guidance, OA CIO's shall ensure that internally facing systems have implemented and attained the requisite e-Authentication assurance level and are using the DOT-issued PIV card for authentication , as required by this guidance.

VIII. Waiver

Requests for waiver from this requirement should be submitted in writing to the DOT Chief Information Officer by the OA Chief Information Officer for consideration and action.

IX. Contact

All questions or comments on this guidance shoulld be directed to the DOT Chief Information Security Officer, Andrew Orndorff, at (202) 366-7111 or via e-mail to andrew.orndorff@dot.gov.