HMCRP

REPORT 6

HAZARDOUS MATERIALS COOPERATIVE RESEARCH PROGRAM

Sponsored by the Pipeline and Hazardous Materials Safety Administration

Feasibility of a Consolidated Security Credential for Persons Who Transport Hazardous Materials

TRANSPORTATION RESEARCH BOARD
OF THE NATIONAL ACADEMIES

TRANSPORTATION RESEARCH BOARD 2011 EXECUTIVE COMMITTEE*

OFFICERS

CHAIR: **Neil J. Pedersen,** *Administrator, Maryland State Highway Administration, Baltimore*
VICE CHAIR: **Sandra Rosenbloom,** *Professor of Planning, University of Arizona, Tucson*
EXECUTIVE DIRECTOR: **Robert E. Skinner, Jr.,** *Transportation Research Board*

MEMBERS

J. Barry Barker, *Executive Director, Transit Authority of River City, Louisville, KY*
Deborah H. Butler, *Executive Vice President, Planning, and CIO, Norfolk Southern Corporation, Norfolk, VA*
William A.V. Clark, *Professor, Department of Geography, University of California, Los Angeles*
Eugene A. Conti, Jr., *Secretary of Transportation, North Carolina DOT, Raleigh*
James M. Crites, *Executive Vice President of Operations, Dallas-Fort Worth International Airport, TX*
Paula J. Hammond, *Secretary, Washington State DOT, Olympia*
Michael W. Hancock, *Secretary, Kentucky Transportation Cabinet, Frankfort*
Adib K. Kanafani, *Cahill Professor of Civil Engineering, University of California, Berkeley*
Michael P. Lewis, *Director, Rhode Island DOT, Providence*
Susan Martinovich, *Director, Nevada DOT, Carson City*
Michael R. Morris, *Director of Transportation, North Central Texas Council of Governments, Arlington*
Tracy L. Rosser, *Vice President, Regional General Manager, Wal-Mart Stores, Inc., Mandeville, LA*
Steven T. Scalzo, *Chief Operating Officer, Marine Resources Group, Seattle, WA*
Henry G. (Gerry) Schwartz, Jr., *Chairman (retired), Jacobs/Sverdrup Civil, Inc., St. Louis, MO*
Beverly A. Scott, *General Manager and CEO, Metropolitan Atlanta Rapid Transit Authority, Atlanta, GA*
David Seltzer, *Principal, Mercator Advisors LLC, Philadelphia, PA*
Lawrence A. Selzer, *President and CEO, The Conservation Fund, Arlington, VA*
Kumares C. Sinha, *Olson Distinguished Professor of Civil Engineering, Purdue University, West Lafayette, IN*
Thomas K. Sorel, *Commissioner, Minnesota DOT, St. Paul*
Daniel Sperling, *Professor of Civil Engineering and Environmental Science and Policy; Director, Institute of Transportation Studies; and Interim Director, Energy Efficiency Center, University of California, Davis*
Kirk T. Steudle, *Director, Michigan DOT, Lansing*
Douglas W. Stotlar, *President and CEO, Con-Way, Inc., Ann Arbor, MI*
C. Michael Walton, *Ernest H. Cockrell Centennial Chair in Engineering, University of Texas, Austin*

EX OFFICIO MEMBERS

Peter H. Appel, *Administrator, Research and Innovative Technology Administration, U.S.DOT*
J. Randolph Babbitt, *Administrator, Federal Aviation Administration, U.S.DOT*
Rebecca M. Brewster, *President and COO, American Transportation Research Institute, Smyrna, GA*
Anne S. Ferro, *Administrator, Federal Motor Carrier Safety Administration, U.S.DOT*
LeRoy Gishi, *Chief, Division of Transportation, Bureau of Indian Affairs, U.S.DOT*
John T. Gray, *Senior Vice President, Policy and Economics, Association of American Railroads, Washington, DC*
John C. Horsley, *Executive Director, American Association of State Highway and Transportation Officials, Washington, DC*
David T. Matsuda, *Deputy Administrator, Maritime Administration, U.S.DOT*
Victor M. Mendez, *Administrator, Federal Highway Administration, U.S.DOT*
William W. Millar, *President, American Public Transportation Association, Washington, DC*
Tara O'Toole, *Under Secretary for Science and Technology, U.S. Department of Homeland Security, Washington, DC*
Robert J. Papp (Adm., U.S. Coast Guard), *Commandant, U.S. Coast Guard, U.S. Department of Homeland Security, Washington, DC*
Cynthia L. Quarterman, *Administrator, Pipeline and Hazardous Materials Safety Administration, U.S.DOT*
Peter M. Rogoff, *Administrator, Federal Transit Administration, U.S.DOT*
David L. Strickland, *Administrator, National Highway Traffic Safety Administration, U.S.DOT*
Joseph C. Szabo, *Administrator, Federal Railroad Administration, U.S.DOT*
Polly Trottenberg, *Assistant Secretary for Transportation Policy, U.S.DOT*
Robert L. Van Antwerp (Lt. Gen., U.S. Army), *Chief of Engineers and Commanding General, U.S. Army Corps of Engineers, Washington, DC*
Barry R. Wallerstein, *Executive Officer, South Coast Air Quality Management District, Diamond Bar, CA*

*Membership as of June 2011.

HAZARDOUS MATERIALS COOPERATIVE RESEARCH PROGRAM

HMCRP REPORT 6

Feasibility of a Consolidated Security Credential for Persons Who Transport Hazardous Materials

Andrew Marinik
Darrell S. Bowman
Ray Pethtel
Tammy Trimble
VIRGINIA TECH TRANSPORTATION INSTITUTE
Blacksburg, VA

Subscriber Categories
Marine Transportation • Motor Carriers • Freight Transportation • Policy

Research sponsored by the Pipeline and Hazardous Materials Safety Administration

TRANSPORTATION RESEARCH BOARD

WASHINGTON, D.C.
2011
www.TRB.org

HAZARDOUS MATERIALS COOPERATIVE RESEARCH PROGRAM

The safety, security, and environmental concerns associated with transportation of hazardous materials are growing in number and complexity. Hazardous materials are substances that are flammable, explosive, or toxic or that, if released, produce effects that would threaten human safety, health, the environment, or property. Hazardous materials are moved throughout the country by all modes of freight transportation, including ships, trucks, trains, airplanes, and pipelines.

The private sector and a diverse mix of government agencies at all levels are responsible for controlling the transport of hazardous materials and for ensuring that hazardous cargoes move without incident. This shared goal has spurred the creation of several venues for organizations with related interests to work together in preventing and responding to hazardous materials incidents. The freight transportation and chemical industries; government regulatory and enforcement agencies at the federal and state levels; and local emergency planners and responders routinely share information, resources, and expertise. Nevertheless, there has been a long-standing gap in the system for conducting hazardous materials safety and security research. Industry organizations and government agencies have their own research programs to support their mission needs. Collaborative research to address shared problems takes place occasionally, but mostly occurs on an ad hoc basis.

Acknowledging this gap in 2004, the U.S. DOT Office of Hazardous Materials Safety, the Federal Motor Carrier Safety Administration, the Federal Railroad Administration, and the U.S. Coast Guard pooled their resources for a study. Under the auspices of the Transportation Research Board (TRB), the National Research Council of the National Academies appointed a committee to examine the feasibility of creating a cooperative research program for hazardous materials transportation, similar in concept to the National Cooperative Highway Research Program (NCHRP) and the Transit Cooperative Research Program (TCRP). The committee concluded, in *TRB Special Report 283: Cooperative Research for Hazardous Materials Transportation: Defining the Need, Converging on Solutions,* that the need for cooperative research in this field is significant and growing, and the committee recommended establishing an ongoing program of cooperative research. In 2005, based in part on the findings of that report, the Safe, Accountable, Flexible, Efficient Transportation Equity Act: A Legacy for Users (SAFETEA-LU) authorized the Pipeline and Hazardous Materials Safety Administration (PHMSA) to contract with the National Academy of Sciences to conduct the Hazardous Materials Cooperative Research Program (HMCRP). The HMCRP is intended to complement other U.S. DOT research programs as a stakeholder-driven, problem-solving program, researching real-world, day-to-day operational issues with near- to mid-term time frames.

HMCRP REPORT 6

Project HM-08
ISSN 2150-4849
ISBN: 978-0-309-21337-0
Library of Congress Control Number 2011933589

© 2011 National Academy of Sciences. All rights reserved.

COPYRIGHT INFORMATION

Authors herein are responsible for the authenticity of their materials and for obtaining written permissions from publishers or persons who own the copyright to any previously published or copyrighted material used herein.

Cooperative Research Programs (CRP) grants permission to reproduce material in this publication for classroom and not-for-profit purposes. Permission is given with the understanding that none of the material will be used to imply TRB, AASHTO, FAA, FHWA, FMCSA, FTA, RITA, or PHMSA endorsement of a particular product, method, or practice. It is expected that those reproducing the material in this document for educational and not-for-profit uses will give appropriate acknowledgment of the source of any reprinted or reproduced material. For other uses of the material, request permission from CRP.

NOTICE

The project that is the subject of this report was a part of the Hazardous Materials Cooperative Research Program, conducted by the Transportation Research Board with the approval of the Governing Board of the National Research Council.

The members of the technical panel selected to monitor this project and to review this report were chosen for their special competencies and with regard for appropriate balance. The report was reviewed by the technical panel and accepted for publication according to procedures established and overseen by the Transportation Research Board and approved by the Governing Board of the National Research Council.

The opinions and conclusions expressed or implied in this report are those of the researchers who performed the research and are not necessarily those of the Transportation Research Board, the National Research Council, or the program sponsors.

The Transportation Research Board of the National Academies, the National Research Council, and the sponsors of the Hazardous Materials Cooperative Research Program do not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the object of the report.

Published reports of the

HAZARDOUS MATERIALS COOPERATIVE RESEARCH PROGRAM

are available from:

Transportation Research Board
Business Office
500 Fifth Street, NW
Washington, DC 20001

and can be ordered through the Internet at:

http://www.national-academies.org/trb/bookstore

Printed in the United States of America

THE NATIONAL ACADEMIES

Advisers to the Nation on Science, Engineering, and Medicine

The **National Academy of Sciences** is a private, nonprofit, self-perpetuating society of distinguished scholars engaged in scientific and engineering research, dedicated to the furtherance of science and technology and to their use for the general welfare. On the authority of the charter granted to it by the Congress in 1863, the Academy has a mandate that requires it to advise the federal government on scientific and technical matters. Dr. Ralph J. Cicerone is president of the National Academy of Sciences.

The **National Academy of Engineering** was established in 1964, under the charter of the National Academy of Sciences, as a parallel organization of outstanding engineers. It is autonomous in its administration and in the selection of its members, sharing with the National Academy of Sciences the responsibility for advising the federal government. The National Academy of Engineering also sponsors engineering programs aimed at meeting national needs, encourages education and research, and recognizes the superior achievements of engineers. Dr. Charles M. Vest is president of the National Academy of Engineering.

The **Institute of Medicine** was established in 1970 by the National Academy of Sciences to secure the services of eminent members of appropriate professions in the examination of policy matters pertaining to the health of the public. The Institute acts under the responsibility given to the National Academy of Sciences by its congressional charter to be an adviser to the federal government and, on its own initiative, to identify issues of medical care, research, and education. Dr. Harvey V. Fineberg is president of the Institute of Medicine.

The **National Research Council** was organized by the National Academy of Sciences in 1916 to associate the broad community of science and technology with the Academy's purposes of furthering knowledge and advising the federal government. Functioning in accordance with general policies determined by the Academy, the Council has become the principal operating agency of both the National Academy of Sciences and the National Academy of Engineering in providing services to the government, the public, and the scientific and engineering communities. The Council is administered jointly by both Academies and the Institute of Medicine. Dr. Ralph J. Cicerone and Dr. Charles M. Vest are chair and vice chair, respectively, of the National Research Council.

The **Transportation Research Board** is one of six major divisions of the National Research Council. The mission of the Transportation Research Board is to provide leadership in transportation innovation and progress through research and information exchange, conducted within a setting that is objective, interdisciplinary, and multimodal. The Board's varied activities annually engage about 7,000 engineers, scientists, and other transportation researchers and practitioners from the public and private sectors and academia, all of whom contribute their expertise in the public interest. The program is supported by state transportation departments, federal agencies including the component administrations of the U.S. Department of Transportation, and other organizations and individuals interested in the development of transportation. **www.TRB.org**

www.national-academies.org

CRP STAFF FOR HMCRP REPORT 6

Christopher W. Jenks, *Director, Cooperative Research Programs*
Crawford F. Jencks, *Deputy Director, Cooperative Research Programs*
Stephan A. Parker, *Senior Program Officer*
Megha Khadka, *Senior Program Assistant*
Eileen P. Delaney, *Director of Publications*
Hilary Freer, *Senior Editor*

HMCRP PROJECT 08 PANEL

Michael C. Smith, *University of Virginia, Charlottesville, VA* (Chair)
John L. Conley, *National Tank Truck Carriers, Inc., Arlington, VA*
W. Scott Hinckley, *Union Pacific Railroad Company, Omaha, NE*
Mark S. Johnson, *International Brotherhood of Teamsters, Washington, DC*
Clyde D. Miller, *BASF Corporation, Florham Park, NJ*
Richard Moskowitz, *American Trucking Associations, Arlington, VA*
Kevin O'Brien, *New York Department of Motor Vehicles, Albany, NY*
Erick-John Saia, *Greenwich Terminals, LLC, Philadelphia, PA*
Paul Bomgardner, *FMCSA Liaison*
Ronald DiGregorio, *PHMSA Liaison*
James Simmons, *PHMSA Liaison*
Steve Sprague, *TSA Liaison*
David Murk, *US Coast Guard Headquarters Liaison*
Joedy W. Cambridge, *TRB Liaison*

AUTHOR ACKNOWLEDGMENTS

The research reported herein was performed under HMCRP Project HM-08 by the Virginia Tech Transportation Institute (VTTI).

Mr. Darrell S. Bowman, leader of the Advanced Technology and Applications Group with VTTI's Center for Truck and Bus Safety, was the project director and principal investigator. The other authors of this report are Andrew Marinik, project associate with the Advanced Technology and Applications Group at VTTI; Ray Pethtel, the university transportation fellow and director of the Transportation Policy Group at VTTI; and Tammy Trimble, project associate with the Advanced Technology and Applications Group at VTTI.

The authors of this report wish to thank Vikki Fitchett and Gene Hetherington for their efforts on this project. The authors would also like to express their gratitude to the members of the project's technical advisory group: Karen Chappell, former deputy commissioner of the Virginia Department of Motor Vehicles; Wiley Mitchell, former senior general counsel of Norfolk Southern Railroad; Dr. Walter Witschey, chairman of the Virginia Rail Policy Institute; Jim Wilding, former president and chief executive officer (CEO) of the Metropolitan Washington Airports Authority; John Smith, executive director of the Virginia Rail Policy Institute; Lieutenant Sal Castruita, operations division lieutenant for the Virginia Port Authority Police Department; and Dale Bennett, president and CEO of the Virginia Trucking Association, for their helpful insight and guidance during this project.

FOREWORD

By Stephan A. Parker
Staff Officer
Transportation Research Board

HMCRP Report 6: Feasibility of a Consolidated Security Credential for Persons Who Transport Hazardous Materials discusses the feasibility of consolidating several existing security credentials, which are necessary under current regulations and policies, into one credential for all transportation modes. The report (1) evaluates the credentialing system to identify duplicative elements and redundant costs and (2) describes the acquisition process, the application elements, and the physical characteristics for each identified credential. In addition, the report identifies the elements of the vetting processes for each credential. An examination of four options for consolidation provides insight into the basic elements of a universally recognized security credential for HazMat transportation workers. The report also identifies key challenges (e.g., impetus and authority, organizational climate, financing, risk, and technological trending) for consolidation of security credentials. Finally, an alternative method of consolidating background checks is identified as a possible intermediate solution for removing duplicative processes and redundant costs. The report will be of interest to policymakers, trade and professional organizations, and other stakeholders involved in transportation credentials for persons who transport hazardous materials.

An evaluation of the data through several key frameworks provides an understanding of the system at its fundamental level.

The security of the nation's HazMat freight in all transportation modes relies on a layered, multi-faceted security program. This comprehensive system is a constant monitor of the many areas, modes, and vehicles involved in HazMat transportation. One important part of this comprehensive security system is credentialing. Security credentials play an important role in ensuring security by vetting those individuals working with, or in support of, HazMat transport. This research project was designed to understand the current security credentialing system within the HazMat transportation system. Furthermore, it was to explore the issues within the credentialing system and, if feasible, evaluate options for a consolidated credential.

Under HMCRP Project HM-08, the Virginia Tech Transportation Institute was tasked to (1) identify credentials and credential elements (the research team used a combination of credentials, credential applications, and literature searching to identify both the credentials and the credential elements); (2) determine time and costs associated with each credential (a questionnaire was designed to collect empirical data related to the time to acquire each credential, while credential cost data were acquired from issuing-agency websites and discussion with issuing-agency representatives); (3) describe the regulatory, policy, and programmatic implications for each credential; (4) determine the feasibility of a consolidated credential for persons who transport hazardous materials; and (5) develop options for

consolidating credentials, based on the potential for a long-term, broadly applicable consolidated credential. This evaluation considered the unique elements and background-check processes of the credentials constituting each option. Further analysis considered the policy and implementation issues associated with consolidating security credentials.

This report and a PowerPoint presentation are available on the TRB website at www.trb.org/SecurityPubs.

CONTENTS

Note: Many of the photographs, figures, and tables in this report have been converted from color to grayscale for printing. The electronic version of the report (posted on the Web at www.trb.org) retains the color versions.

SUMMARY

Feasibility of a Consolidated Security Credential for Persons Who Transport Hazardous Materials

Introduction

The safe transport of hazardous materials (HazMat) throughout America's transportation infrastructure (to include points of origin and destination) is imperative to a safe and economically robust society. The security of the nation's HazMat freight in all transportation modes relies on a layered, multi-faceted security program. This comprehensive system is a constant monitor of the many areas, modes, and vehicles involved in HazMat transportation. One important part of this comprehensive security system is credentialing. Security credentials play an important role in ensuring security by vetting those individuals working with, or in support of, HazMat transport. This research project was designed to understand the current security credentialing system within the HazMat transportation system. Furthermore, it was to explore the issues within the credentialing system and, if feasible, evaluate options for a consolidated credential.

Research Approach

The research team used an evolutionary approach to this project in which each task provides the foundation for the following tasks. The research team evaluated each credential at its most basic level to determine the elements that make up the credential and the credentialing process. This elemental analysis approach provided the data blocks necessary for generating and evaluating consolidated credential options in Phase II. The research team performed the following tasks during Phase I:

- Task 1. Identify credentials and credential elements.
  - The research team used a combination of credentials, credential applications, and literature searching to identify both the credentials and the credential elements.
- Task 2. Determine time and costs associated with each credential.
  - To accomplish Task 2, a questionnaire was designed to collect empirical data related to the time to acquire each credential. This questionnaire was an online survey posted for approximately 10 weeks. Credential cost data were acquired from issuing agency Web sites and discussion with issuing agency representatives.
- Task 3. Understand the regulatory, policy, and programmatic implications for each credential.
  - Regulatory analysis data collection focused on the Code of Federal Regulations, the United States Code, the Federal Register, and issuing agency Web sites. The research team also contacted the issuing agencies for clarification when necessary.
- Task 4. Determine the feasibility of a consolidated credential for persons who transport hazardous materials.

– The research team used the strengths, weaknesses, opportunities, and threats (SWOT) analysis framework to determine the feasibility of a consolidated credential approach. Both a consolidated credential approach and a non-consolidated credential approach were analyzed from the perspectives of security and cost-effectiveness.

In Phase II, the research team developed four options for consolidating the credentials, based on the credentials deemed as candidates for consolidation in Phase I. Each of the four options was evaluated for potential as a long-term, broadly applicable consolidated credential. This evaluation considered the unique elements and background check processes of the credentials comprising each option. Further analysis considered the policy and implementation issues associated with consolidating security credentials.

Findings

The credential synthesis and elemental analysis, time and cost analysis, and regulatory analysis resulted in the identification of 19 credentials required of persons who transport hazardous materials:

- Transportation Worker Identification Credential (TWIC);
- Merchant Mariner License (MML);
- Merchant Mariner Document (MMD);
- Merchant Mariner Credential (MMC);
- Standards of Training, Certification, and Watchkeeping for Seafarers (STCW);
- Florida Uniform Port Access Credential (FUPAC);
- Local Port IDs;
- Security Identification Display Area (SIDA) badge;
- Pilot's License;
- e-RAILSAFE;
- Engineer's License
- Commercial Driver's License with HazMat Endorsement (CDL-HME);
- Free and Secure Trade (FAST) card;
- United States Postal Service (USPS) credential;
- NEXUS;
- Secure Electronic Network for Travelers Rapid Inspection (SENTRI);
- U.S. passport;
- RAPIDGate; and
- Common Access Card (CAC).

All of the identified credentials were categorized as either safety credentials, security credentials, or dual credentials by primary function or purpose. Credentials with a primary purpose of validating the credential-holder's skill set were deemed safety credentials. Credentials whose primary function is to vet the credential-holder and confirm identity were deemed security credentials. Those credentials that functioned as a secure form of identification while ensuring that the credential-holder possesses the necessary skills were deemed dual credentials. Four safety credentials (i.e., MML, STCW, Pilot's License, and Engineer's License) were not carried on through the analysis because the consolidation of skill requirements was infeasible. Two security credentials (i.e., e-RAILSAFE and RAPIDGate) were identified by Task 2 questionnaire responses. These two credentials are administered by private companies, thus they were not considered in any analyses due to being outside the scope of the project. Although FUPAC has broader applicability than most Port IDs due to acceptance

at all ports throughout Florida, it was ultimately treated as a Local Port ID. All Local Port IDs were dropped from further analysis because the Local Port IDs are controlled by the individual port authorities and were deemed too varied to aggregate elemental data in a meaningful way.

Therefore, the elemental and cost analyses included 9 security credentials and 2 dual credentials, for a total of 11 credentials (i.e., CAC, CDL-HME, FAST, MMD, MMC, NEXUS, passport, TWIC, SENTRI, SIDA, and USPS) that were deemed candidates for total consolidation. Elemental analysis of the 11 credentials resulted in the identification of 91 elements. The results were split into requirements-to-obtain credential (i.e., those pieces of information necessary to get the credential) and attributes (i.e., those pieces of information provided by the credential). There were 64 unique requirements-to-obtain elements and 27 unique attribute elements. All 11 candidate credentials shared five of the requirements-to-obtain elements, and three attribute elements. Seven of the requirements-to-obtain elements and four of the attribute elements were applicable to over 90% of the credentials. In all, 25 elements (10 attribute elements and 15 requirements-to-obtain elements) apply to over 50% of the candidate credentials.

The 11 candidate credentials ranged in cost from $50.00 (for the FAST and NEXUS credentials) to $132.50 (for the TWIC). The CDL-HME is issued by each state and the District of Columbia, with unique costs in each location ranging from a low of $107.25 (North Dakota) to a high of $326.25 (New York).

The questionnaire resulted in 378 respondents over a 10-week collection period. Respondents ranged in age from less than 25 to 74 years old. The largest percentage (41%) fell within the bracket of 45 to 54 years old. Approximately 33% of respondents have been involved in the transportation of hazardous materials for more than 25 years. Of the responses received, 323 respondents held a CDL-HME, 247 respondents held a TWIC, and 52 respondents held a FAST card. No other credential was identified as being held by more than 10 respondents.

The respondents reported that the time to acquire a credential ranged from less than 2 weeks to more than 16 weeks. The largest percentage (34%) identified that their time to acquire was between 2 and 4 weeks. Eighty-two percent of the respondents reported acquiring their credential in less than 8 weeks. When questioned on their perception related to the time to acquire credentials on a five-point Likert-type scale (possible responses being *way too short, too short, about right, too long,* and *way too long*), 40% thought the time was *about right.* Approximately 39% thought the time to acquire was *too long.* In addition, 63% of respondents reported that it took less than 2 hours to complete the application for the credentials they held. Seventy-five percent of respondents reported that the time to complete the credential application was *about right.* With regard to physically acquiring the credentials, 75% of respondents reported that it took less than 2 hours to pick up their credentials. Sixty-four percent of respondents felt that the time to physically acquire the credentials was *about right.*

A SWOT analysis was done from both a security perspective and a cost-effectiveness perspective on both a consolidated credential approach and a non-consolidated credential approach. The security perspective SWOT analysis identified eight strengths and opportunities for a consolidated credentialing approach including

- Provides one credential for end-user,
- Has uniform look and design on the credential,
- Ensures a minimum threshold for security,
- Simplifies training for security personnel,
- Simplifies “threats to mitigate” list,
- Ensures only one issuing agency to notify if problems arise,
- Fosters ability to quickly adapt policy for new threats, and
- Enables better tracking of applicants.

The security perspective SWOT analysis also identified five weaknesses and threats for a consolidated credentialing approach including

- Institutional resistance,
- State and federal legislative actions required,
- Increased ability to abuse/misuse,
- Decreased resolution with regard to the "threats to mitigate" list, and
- International issues.

The cost-effectiveness perspective SWOT analysis yielded four strengths and opportunities related to the consolidated credential approach, including

- Eliminates redundancies for the issuing agencies,
- Eliminates redundancies for the credential users,
- Increases availability of enrollment centers, and
- Decreases training requirements for security personnel.

The cost-effectiveness perspective SWOT analysis also identified the following weakness related to the consolidated credential approach, including

- Requires new or additional technology.

The SWOT analysis of a non-consolidated credential approach was done from both a security perspective and a cost-effectiveness perspective. The security perspective SWOT analysis identified two strengths and opportunities for a non-consolidated credential approach including

- Provides tailored credentialing and
- Enables focused applicant assessment.

Six weaknesses and threats also were identified, including

- Inconsistent vetting processes,
- Re-vetting of the same people,
- Inefficient information and data collection,
- Data collection or processing errors,
- Complexity of information sharing, and
- Variance in credential appearances.

In the same manner as the consolidated credential approach, a SWOT analysis was done from a cost-effectiveness perspective for the non-consolidated approach. This SWOT analysis did not identify any strength or opportunity, but it did identify four weaknesses and threats, including

- Increases administrative costs,
- Requires multiple enrollment centers and forms,
- Requires multiple credential costs, and
- Requires more training for facility security personnel.

The collective results of the SWOT analysis indicate that a consolidated credential approach would be desirable as compared to a non-consolidated approach. Additionally, the results of

the SWOT analysis are the foundation on which a consolidated credentialing system should be designed. A consolidated credential approach should take advantage of the existing strengths while exploiting the identified opportunities where possible and, at the same time, mitigate the weaknesses and focus on preventing the threats.

The findings of the Elemental Analysis, the Time and Costs Analysis, the Regulatory Analysis, and the SWOT Analysis indicated that the consolidation of several security credentials required of persons who transport hazardous materials was feasible, including: TWIC, MMD, SIDA, USPS, and CAC. Based on the Phase I data collection efforts, the use cases, and technical advisory group (TAG) input, four consolidated credential options were developed. These consolidation options included

- Option 1—TWIC;
- Option 2—TWIC, MMD, SIDA, USPS, and CAC;
- Option 3—TWIC and MMD; and
- Option 4—TWIC, SIDA, CAC, and MMD.

These options were then evaluated through assessment of their collective elements and background check processes. The credential combination with the most promise for broad applicability would be the option with the greatest number of unique elements. This assumes each element is necessary for each credential, and functionality would be limited without a given element. The comparison of these options did, however, provide some perspective as to the relative differences between them. Option 1 was, in fact, not a consolidated effort, but more of an evaluation of one credential (TWIC) as it compares to the other consolidated efforts. This provided a lower bounding of the unique elements necessary to create a transportation security credential. Option 2 included all credentials deemed feasible for consolidation providing an upper bounding of unique elements. Option 3 consisted of those credentials (deemed feasible for consolidation) specific to the marine mode and allowed for evaluation of the elemental variance for consolidating within one mode. Option 4 consisted of all credentials determined feasible for consolidation excepting the USPS credential. It was determined that this credential was reported infrequently and did not appear to play a major role in the transportation of hazardous materials. Therefore, Option 4 was used to evaluate the impact of the USPS credential on the set of elements and associated background checks for consolidation.

Evaluation of the background check process was similar and, in fact, was evidence of even greater alignment across all options. This near harmony of already existing processes indicates a high chance of success in eliminating redundancy as it relates to security credential background check processes.

This evaluation did not consider issues of implementation or legislative impetus associated with the consolidation process. These issues were reviewed independently using a multiple-perspective analysis. This analysis considered the challenges associated with policy implementation as related to the consolidation of security credentials for persons who transport hazardous materials.

Conclusions

There are a number of redundant elements within the HazMat transportation worker security credentialing system. For at least several credentials (e.g., TWIC, MMD, SIDA, USPS, and CAC) consolidation is a feasible alternative. However, there is a significant amount of information that must be fully understood, and it is imperative to gain stakeholder input from all levels. The development and implementation of a consolidated security credential will

require the preservation of unique features of the individual credential while creating a universally applicable credential (within the HazMat transportation system).

The research also suggests that consolidation of background checks (the vetting processes) could be achieved and may present an intermediate alternative while still exploring the consolidation of full credentials. The majority of the credentials identified as security credentials for transporting hazardous materials require a very similar background investigation. Through data-sharing agreements and standardization of the adjudication process, a streamlined background investigation for these credentials could be achieved. This alternative also would require a standardization of the disqualifying offenses.

It is recommended that further research be done to completely identify and understand the costs and benefits associated with the consolidation process. This cost information is imperative to truly determine the value of a consolidated option in regard to the existing credentialing system. Furthermore, it is recommended that a separate effort be undertaken to focus on the potential standardization of background evaluations for credentials. This effort appears most promising in increasing efficiency and decreasing costs in the short term.

CHAPTER 1

Background

Since the terrorist attacks of September 11, 2001, transportation security has been a major focus for policymakers, the transportation industry, and the general public. Because the U.S. air, land, and marine transportation systems are designed to promote commerce through accessibility and efficiency, they are highly vulnerable to terrorist attack.(*1*) Every day, an estimated 6 million workers, including longshoremen, mechanics, aviation and railroad employees, and truck drivers, access secure areas of the nation's estimated 4,000 transportation facilities while performing their jobs. Some of these workers, such as truck drivers, regularly access secure areas at multiple transportation facilities.(*2*)

Of particular security concern are those workers who are involved in the transportation of hazardous materials. According to *TRB Special Report 283: Cooperative Research for Hazardous Materials Transportation: Defining the Need, Converging on Solutions,*(*3*) the U.S.DOT has estimated that about 817,000 shipments consisting of 5.4 million tons of hazardous materials are made daily in the United States, which would total nearly 300 million shipments and 2 billion tons of hazardous cargo per year. The safekeeping of hazardous materials in transit is paramount to the safety and security of people everywhere. Vetting the personnel working with and around hazardous materials through a credentialing process is essential for a successful transportation security management program.

However, the U.S. credentialing process, as established by the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), the Maritime Transportation Security Act of 2002 (MTSA), and the Safe Port Act of 2006, lacks a coordinated vision and fails to recognize the multimodal and intermodal nature of the transportation sector.(*4*) This disjointed vision has created a fragmented security credential system that requires various security credentials throughout the transportation logistics chain. Admiral James M. Loy, formerly of the Transportation Security Administration (TSA) and Department of Homeland Security (DHS), commented that there are instances when truck drivers may have as many as 23 identification (ID) cards at any given time while involved in the transportation of hazardous materials.(*4*) For example, a truck driver hauling hazardous materials would be required to hold a Hazardous Materials Endorsement (HME), present a Security Identification Display Area (SIDA) badge before entering an airport, display a Common Access Card (CAC) while accessing a Department of Defense facility, show a Free and Secure Trade (FAST) credential for priority border crossings, and present a Transportation Worker Identification Credential (TWIC) when entering a maritime port. Each of these credentials involves similar background checks but requires workers to submit separate applications and duplicative fees. In response to the current situation, the Small Business Administration (SBA) has placed this issue on its Top 10 list of burdensome federal regulations. The SBA has asked TSA to revise its regulations to waive the background check for an HME applicant who holds a valid TWIC. According to SBA, this requirement for redundant background checks costs the individual applicants nearly $100 and costs the trucking industry up to $30 million annually.(*5*) This scenario is not unique for truck drivers but is experienced by many other workers involved in the transport of hazardous materials. Each credential has costs—both monetarily and in required time to acquire—that result in duplicative costs and additional time required of both the credentialing agency and the person requesting credentialing. These costs provide a strong incentive to consolidate the transportation security credentialing system and investigate the feasibility of what, from a user's perspective, would be a single, uniform credential for HazMat transportation security.

The research objective of this project is to perform a detailed evaluation of the HazMat transportation worker credentialing

system to identify duplicative elements and redundant costs throughout the process. The key outcome of the project will be determining the feasibility of consolidating many, or all, of the existing local, state, and federal credentials necessary under current regulations and policies, into one credential for all transportation modes that is cost-effective and maintains an equal or greater level of security and safety. This consolidated credential will establish a worker's identity, eligibility to access secure areas, and eligibility to obtain or hold transportation-related licenses, credentials, and other government certifications required of persons who transport hazardous materials by all modes in the United States.

CHAPTER 2

Research Approach

This research was done in a multi-phase approach. The main goal of Phase I was to understand the existing credentialing system as it relates to persons who transport hazardous materials, and determine the feasibility of a consolidated credential within that system. This first phase involved the examination of the current credentialing processes at their basic levels to understand each credential's elements (e.g., security attributes, related costs, time to acquire) and associated strengths and weaknesses. This elemental analysis approach provided the data blocks necessary for generating and evaluating consolidated credential options in Phase II.

Phase II was dependent on the results of Phase I and the feasibility of consolidating credentials. Phase II consisted of a single task to develop potential options for consolidating credentials for persons who transport hazardous materials, and evaluating the strengths and weaknesses associated with each potential option. Tasks were organized as follows (note, Task 5 was to produce the interim report and is not considered part of the research approach for Phase I):

- Task 1 (Phase I)
  - Identify credentials and credential elements.
- Task 2 (Phase I)
  - Conduct time and cost analysis.
- Task 3 (Phase I)
  - Conduct regulatory analysis.
- Task 4 (Phase I)
  - Determine feasibility of consolidation.
- Task 6 (Phase II)
  - Develop and evaluate options for consolidation.

Phase I

The research team developed and followed the flow chart shown in Figure 2-1 to complete Phase I tasks. After identifying the credentials, the research team analyzed data in three key areas: Elemental Analysis, Time and Cost Analysis, and Regulatory Analysis.

Credential Synthesis

The research team compiled all security credentialing literature in the Virginia Tech Transportation Institute (VTTI) HazMat library. This effort was supplemented by a national and international review of Internet resources, academic articles, and other public information sources with the objective of determining the underlying credentialing processes and regulatory requirements for each credential.

To augment the information, the research team assembled a technical advisory group (TAG). The group was comprised of seven members with varied experience in the different modes of transportation or credentialing. Each TAG member was selected because of a direct role or related experience with credentialing and is listed below with a brief description of their relevance to this effort.

- John Smith has applied for, and used, HazMat credentials and is familiar with the application process.
- Karen Chappell is responsible for the state issuance and regulation of HazMat credentials.
- Lt. Sal Castruita is on the security team of the Virginia Port Authority.
- Wiley Mitchell was selected because of his understanding and knowledge of the purpose of the legal aspects of credentialing for the Norfolk Southern Railroad.
- Jim Wilding was chief executive officer (CEO) of the Metropolitan Washington Airports Authority and is aware of the risks involved and the reasons for credentials that are necessary in order to access commercial airports.
- Walter Witschey is the current president of the Virginia Rail Policy Institute and has access to numerous individuals and organizations associated with the freight rail industry.
- Dale Bennett is the president of the Virginia Trucking Association and has access to carriers and drivers involved in HazMat shipping.

A short biography of each member is provided in Appendix A.

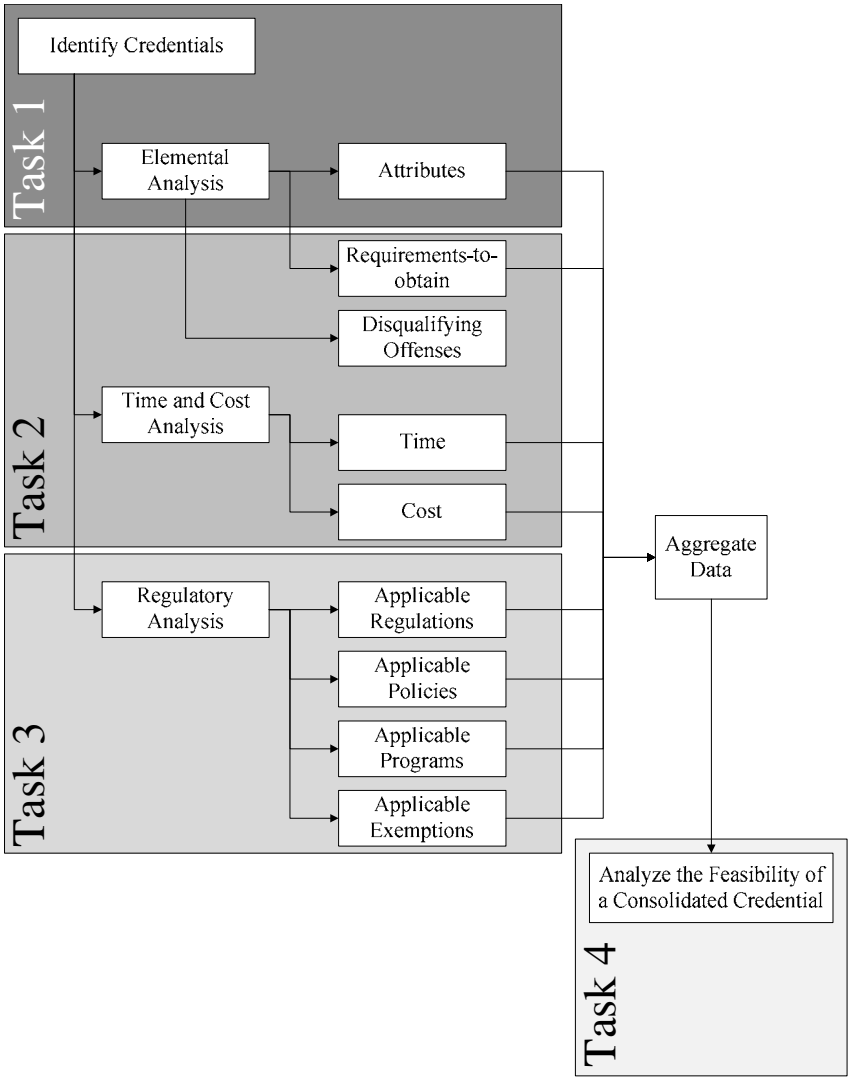

Figure 2-1. Research approach for Phase I.

Elemental Analysis

With a completed list of relevant credentials, the research team focused on identifying the elements of each. Elements are individual pieces of information used to acquire a credential, or contained within a credential to communicate the necessary information to authenticate the identity of the credential holder. Examples of elements are full name, address, access level, date of birth, photograph, and biometric attributes. To identify the elements, the research team focused on two key sources—the application for, and a representation of, the actual credential.

The application for each credential was used to determine the requirements-to-obtain elements for that credential. Many of the credentials' applications were readily available on the issuing agencies' Web sites. However, the research team also obtained more obscure applications through companies that have applied for these credentials in the past; in one case, the research team actually completed the online application process. For two of the identified credentials, the Commercial Driver's License (CDL)-HME and SIDA, the Code of Federal Regulations (CFR) was used to capture the minimum requirements. These federal minimums were used to provide a common denominator because each credential is handled by multiple issuing agencies (i.e., the states for a CDL-HME, and the airports for a SIDA).

To obtain the attribute elements, the research team used a combination of photographs of credentials, actual credentials, and written descriptions of credentials to identify each attribute element on each credential. The collected elemental data were placed in matrices to visually represent the data and to track gaps in the data throughout the progression of the research. This added a level of redundancy in the research approach to ensure all available data were captured.

Time and Cost Analysis

Although time and costs both provide an understanding of the burden to acquire security credentials, it was necessary to perform two separate data collection efforts. First, the research team developed a questionnaire to collect time-related data from actual credential holders. Second, the research team collected pricing data from each issuing agency related to each credential.

Consolidated Credential Questionnaire

Since this was an examination of several security credentials across many transportation modes, a survey was designed that would allow for the analysis of the credentials themselves, as well as the use of the credentials across modes. The resulting survey addressed the following modes: air, highway and tractor-trailer, marine, and rail. Additionally, the following security credentials were explored:

- CDL-HME,
- TWIC,
- FAST,
- Florida Uniform Port Access Credential (FUPAC),
- Merchant Mariner Credential (MMC),
- Merchant Mariner Document (MMD),
- Merchant Mariner License (MML),
- NEXUS,
- Secure Electronic Network for Travelers Rapid Inspection (SENTRI), and
- SIDA.

The questionnaire was developed to ensure that the broadest range of responses could be accommodated. This approach provided an understanding of the time required to obtain the aforementioned credentials.

The questionnaire was created through collaboration with the TAG. During the developmental stage, the VTTI team conferred several times with the TAG to discuss questionnaire design and format. Discussions ranged from general questionnaire goals and outlines to specific question methodology. Throughout the process, the team members exchanged questionnaires and ideas in order to determine the best approach for obtaining the desired information.

Credential Costs

To collect the credential cost data, the research team collected the most up-to-date pricing information available using data from the Web sites of the issuing agencies. These data were organized by credential and placed into a matrix similar to those used for the elemental analysis. Many of the identified credentials were federally issued, therefore, a single cost was associated with each. However, the CDL-HME is a state-issued credential and its cost varies by state. These data were publicly available from each state and placed into the matrix along with the federally issued credentials. The SIDA costs are designated by the issuing airport authority and, due to variability, are captured as a mean of several agency-reported costs in the cost results matrix.

Regulatory Analysis

To fully understand the credentialing process, the team researched the regulatory authorities, programs, and policies, and any applicable exemptions for each credential. This was done by a review of the CFR and the United States Code (U.S.C.), where applicable to each credential. When necessary, local regulations were consulted to understand the authorities for credentials that are not federally issued. After identifying the authorities and programs associated with each credential, the team investigated policy- and program-specific Web sites. Furthermore, where necessary, the research team contacted representatives of the credential-issuing agencies for clarification or additional information.

SWOT Analysis

A strengths, weaknesses, opportunities, and threats (SWOT) analysis is designed to aid in the strategy decisions related to change in an organizational effort. This technique was used to analyze the advantages and disadvantages of a consolidated and a non-consolidated security credentialing approach for persons who transport hazardous materials. The advantage to the SWOT analysis is the defined manner in which the data are examined, ensuring analysis from both internal (i.e., processing of the credential) and external (i.e., use of the credential) points of view (Figure 2-2). The research team used the

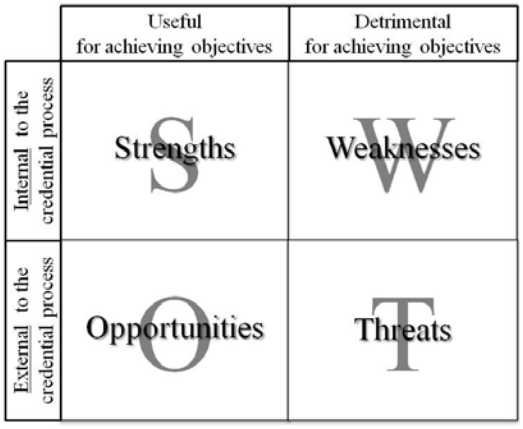

Figure 2-2. SWOT analysis.

information from Tasks 1, 2, and 3 to complete the SWOT analyses of both consolidated and non-consolidated credential approaches.

It was necessary to examine the approach for a consolidated credential rather than the result of a consolidated credential to understand the issues from a relative perspective. The feasibility of a consolidated credential requires change from the existing system, not the development of a completely new credentialing system (i.e., an absolute perspective). Therefore, the SWOT analysis evaluated the process of moving to, and use of, a fitting consolidated credential.

The research team evaluated the feasibility of a consolidated credential from two different perspectives (i.e., security and cost-effectiveness) and from two different outcomes (i.e., consolidated credential and non-consolidated credential). This resulted in four unique SWOT analyses focusing on each perspective and assuming each outcome. Therefore, a SWOT analysis was done for each of the following conditions:

- Consolidated credential—security perspective,
- Consolidated credential—cost-effectiveness perspective,
- Non-consolidated credential—security perspective, and
- Non-consolidated credential—cost-effectiveness perspective.

After completing all four SWOT analyses, the research team provided the results and associated assumptions to members of the TAG. The TAG was tasked with evaluating the results, assumptions, and conclusions, and providing feedback. All comments received from the TAG were discussed with the commenting TAG member and incorporated into the results. The results and specifics regarding assumptions for each SWOT analysis are provided in Chapter 3.

Phase II

The Phase II effort built upon the results of the previous phase by limiting considerations for consolidation to only those results that were deemed applicable to consolidation. The results indicated that additional data collection efforts were necessary to accomplish the final task of determining and evaluating the options for credential consolidation. These supplementary efforts involved evaluating credential usage at ports, and developing use-cases to provide insight into several applicants' actual experiences (e.g., cost and time) in regard to applying for, and receiving, security credentials.

Evaluation of Port Credential Usage

This effort consisted of contacting a sample of ports throughout the United States and determining if they were currently using any credentials (i.e., local port identification) in addition to the federally mandated TWIC. This effort was designed to provide some insight into the propensity of local authorities to adopt new requirements and replace existing systems versus adopting the mandated requirements as an additional layer of security. The results of this effort are indicative of potential success with consolidation of existing security credentials under local and state authorities, as well as for federally managed security credentials.

Use Cases

The results of the Phase I, Task 2 effort to understand time and cost information related to the users of security credentials provided high-level understanding of the system. However, it was evident that several in-depth case reviews could be beneficial to characterizing the system as well. This effort followed up on the previous effort to better understand the burdens of several users, the results of which provide some insight into the microeconomic burdens in specific cases.

Consolidated Credential Options and Evaluation

Security credentials are just one part of the HazMat transportation security system. Figure 2-3 provides a high-level overview of the credentialing process. Threats to the system arise when individuals with malicious intent are able to create an unsafe situation. To prevent these threats, the system must ensure (to the extent possible) that all personnel entering the protected area are well-intentioned. This is accomplished by two distinct processes. The vetting process, which takes place during the credential acquisition process, ensures that the applicant exhibits no indication of malicious intent and could have real and proper reasons for accessing the areas protected by the credential. The communication process allows the entry point personnel, with the aid of technology systems, to verify that the current credential-holder has successfully been vetted.

Both processes must perform appropriately for the HazMat transportation security system to be effective. If the vetting process fails, a valid credential-holder may gain access to secure areas with intentions of deviant behavior. Conversely, should the communication aspect fail, the person presenting the security credential may fraudulently enter secure areas, again with intentions of harm. Therefore, all security credential processes should strive to be as thorough as possible in vetting the credential-holder, and as accurate as possible when communicating the identity.

The effectiveness of security credentials can be evaluated through a variety of methods. The appropriateness of each method depends upon the end goals of the credentials' administrators. For example, one could track the number of security breaches related to security credential failures, or the number of issues associated with the vetting and communication

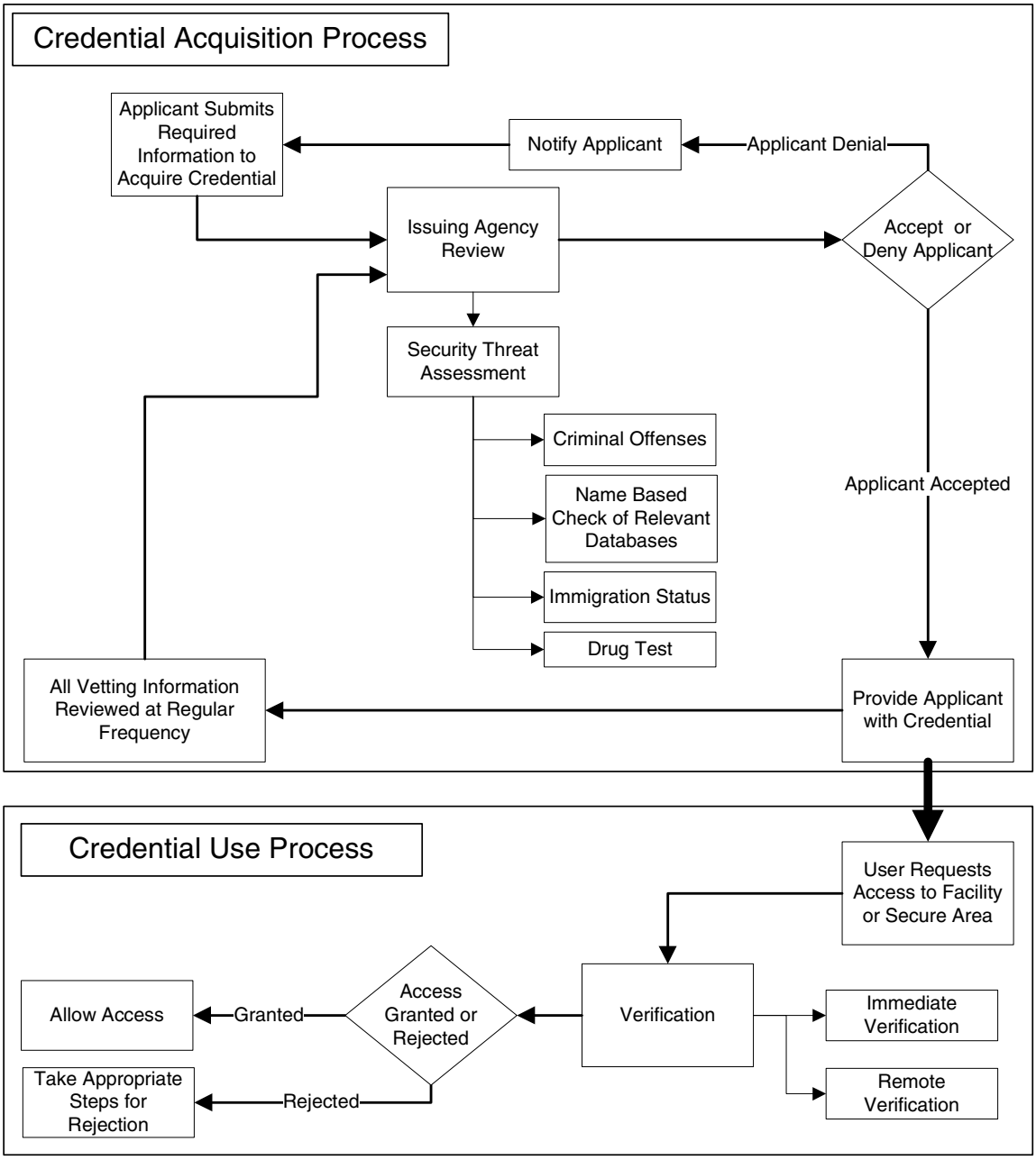

Figure 2-3. Application and use processes for security credentials.

processes. However, because the vetting and communication processes take place within a larger interconnected system, each method, when taken alone, may not accurately reflect the effectiveness of the credential. Within the HazMat transportation system there are multiple types of facilities, areas, and border crossings requiring security. At each entry gate, the transportation worker must prove that he/she holds a valid security credential. In many cases, the security credential is specific to the facility (area or border crossing) and the issuing agency with jurisdiction. This specificity has created a complex system of many secure facilities and an equivalent number of security credentials. Additionally, many transport workers frequently access multiple facilities under various oversight agencies and, thus, are required to utilize multiple credentials to perform their job requirements.

A proposed solution for simplifying the complex credentialing system with regard to HazMat transportation is to eliminate or reduce redundancies. Many secure areas within the HazMat transportation system rely on the same basic strategy of using security credentialing to protect the infrastructure, personnel, and business integrity within system operations. Consolidating some or all of the security credentials (or minimizing redundancies) can be beneficial for all stakeholders. Consolidation could result in lowered costs

related to operating a HazMat transportation-related business and lowered costs associated with securing key areas, facilities, and border crossings. Additionally, by increasing efficiency related to security credentialing, the costs associated with vetting credential applicants and training security personnel can be decreased.

The consolidation of security credentials must maintain the highest level of security afforded by the individual credentials that were merged. Many of the existing credentials are issued by different agencies and cover different modes of transportation. A universally applicable, fundamentally secure credential requires certain traits that must be agreed upon by each of the issuing agencies as well as the end users.

Therefore, the Phase II effort consisted of developing several options for consolidation, and evaluating such options based on collected data. These options were developed based on the results of elemental analysis, survey data, and use cases. They were then evaluated for potential as a successful, broadly applicable, consolidated credential. The evaluation considered the basic building blocks (unique elements consistent with candidate credentials comprising each option) and the unique background check processes required to accomplish each option.

Policy Implementation Analysis

Successful policy implementation is, in part, determined by the nature of the policy problem. Three types of policy problems exist: well-structured problems, moderately structured problems, and ill-structured problems. Ill-structured policy problems are those policy problems that typically include many different decision makers whose utilities (values) are either unknown or impossible to rank in a consistent manner.(*6*) When evaluating well-structured and moderately structured policy problems, preferences that are transitive in nature (e.g., Policy A1 is preferable to Policy A2 and Policy A2 is preferable to Policy A3; therefore, Policy A1 is preferable to Policy A3) can be ascertained. However, ill-structured problems are intransitive in nature and the best or most appropriate solution is often difficult to determine. Ill-structured policy problems include many decision makers, an unlimited number of alternatives, conflicting utilities (values), unknown outcomes, and incalculable probabilities. Additionally, ill-structured problems present complex choices that make it difficult to make a satisfactory recommendation that combines the values of all the stakeholders. As a result, the evaluation of alternative consolidated credential options requires the use of methods appropriate for the evaluation of ill-structured policy problems.(*6*)

The team used multiple-perspective analysis to obtain increased insight into potential implementation problems and solutions. Multiple-perspective analysis was designed to be an alternative to rational-technical approaches and was designed specifically for the analysis of ill-structured policy problems. The multiple-perspective analysis method allows researchers to systematically evaluate problem situations through the use of organizational, technical, and personal perspectives. The major features of each perspective, as defined by Dunn (*6*), are as follows:

- Organizational perspective: Relies on standard operating procedures, rules, and institutional routines. Problems and solutions are viewed as part of an orderly progression from one organizational state to another.
- Technical perspective: Requires objective analysis and a scientific-technological worldview. Problems and solutions are viewed in terms of optimization models and incorporate ideas drawn from probability theory, benefit-cost and decision-making analysis, econometrics, and systems analysis.
- Personal perspective: Emphasizes intuition, leadership, and self-interest as factors governing policies and their impacts. Problems and solutions are viewed in terms of individual perceptions, needs, and values.

Through the use of a multiple-perspective analysis, the proper balance of each perspective can be preliminarily determined. This determination will aid in the final development of options for a consolidated credential.

CHAPTER 3

Findings and Applications

Identified Credentials

The literature search, in combination with TAG advisement, resulted in identification of 19 credentials related to persons who transport hazardous materials. For many of these credentials, their applicability extends beyond the transport of hazardous materials; however, each credential identified was required of a person who transported hazardous materials across the various transportation modes. Two of the credentials (i.e., e-RAILSAFE and RAPIDGate) are administered by private entities but were included in Table 3-1 because they were identified by the Task 2 questionnaire. These two credentials were not considered in any further analyses. Table 3-1 lists the credential name, acronym or abbreviation (if applicable), issuing agency, and primary transportation mode (other transportation modes may be applicable in some cases).

By transportation mode, seven credentials were designated for marine, seven credentials were designated for highway, two credentials were designated for air, and two credentials were designated for rail. One credential, the U.S. passport, was considered equally applicable to all transportation modes. Figure 3-1 shows the chronological progression of the credentials based on the first year of issuance (or, in some cases, the date of legislation first mentioning the program).

Due to multiple authorities issuing U.S. passports, in 1856 Congress enacted legislation providing full authority to the State Department to be the only legal entity to issue U.S. passports.(*7*) In 1938, the United States Merchant Marine Academy was founded and became the first federal government entity to issue the Merchant Mariner License. By 1941, the Defense Entry and Departure Act required U.S. citizens to use a passport when traveling abroad. In 1978 in London, the International Maritime Organization (IMO) adopted the International Convention on Standards of Training, Certification, and Watchkeeping for Seafarers (STCW). The IMO adopted a major STCW revision in 1995.

The Commercial Driver's License (CDL) was first introduced in 1986 through the Commercial Motor Vehicle Safety Act of 1986 (CMVSA), and did have restrictions on the operation of commercial motor vehicles (CMVs) transporting hazardous materials. These restrictions were knowledge- and capability-based, and did not include a threat assessment. Although the CMVSA was enacted in 1986, it was not until 1992 that drivers were required to have a CDL to operate some vehicles.(*8*) SENTRI was first introduced in 1995 as a method of increasing security and efficiency at border crossings. The NEXUS program was next introduced in 2002 as a highway-specific program for pre-screening individuals for greater efficiency at border crossings. In the same year, SIDA badges were introduced as a measure of security in airports. Several acts of legislation in 2002 added new credentials or additional security programs to existing credentials, including the USA PATRIOT Act and the MTSA of 2002 (refer to the regulatory analysis section for specifics). In 2003, to acquire an HME for a CDL began requiring a full security threat assessment. In 2004, USPS published a management instruction indicating the necessary steps for screening highway transportation contract employees.(*9*) Also in 2004, the Florida State Legislature passed a bill enacting the FUPAC (Title 22 Ports and Harbors, Ch. 311, Sec. 311.125 Florida Statutes). The FAST program and card were first implemented in 2005, based on the Trade Act of 2002. The FAST card is designed to add a pre-screened layer of security to cross-border highway freight transportation.(*10*) In 2006, the U.S. military began issuing the CAC to contractors accessing their facilities, including truck drivers who may be hauling hazardous materials. By 2007, the NEXUS program was extended to include air transportation, although the intent of the program was relatively unchanged. In 2007, the SIDA badge vetting process was changed to include the TSA security threat assessment prior to issuing a badge (as opposed to the original process of the airport issuing the badge before providing TSA with the information to perform the security threat assessment).(*11*) By 2009, both the MMC and the TWIC had

Table 3-1. Identified credentials related to hazmat transportation workers.

Name	Acronym	Issuing Agency	Mode
Transportation Worker Identification Credential	TWIC	TSA	Marine
Merchant Mariner License	MML	United States Coast Guard (USCG)	Marine
Merchant Mariner Document	MMD	USCG	Marine
Merchant Mariner Credential	MMC	USCG	Marine
Standards of Training, Certification, and Watchkeeping for Seafarers	STCW	International Maritime Organization/USCG	Marine
Florida Uniform Port Access Credential	FUPAC	Florida Department of Highway Safety and Motor Vehicles	Marine
Local Port IDs	N/A	Local Port Authority	Marine
Security Identification Display Area Badge	SIDA	Individual Airport Authorities	Air
Pilot's License	N/A	FAA	Air
e-RAILSAFE	N/A	e-VERIFILE.COM, Inc.	Rail
Engineer's License	N/A	FRA	Rail
Commercial Driver's License with HazMat Endorsement	CDL-HME	States/TSA	Highway
Free and Secure Trade Card	FAST	Customs and Border Protection (CBP)	Highway
United States Postal Service Credential	USPS	United States Postal Service (USPS)	Highway
NEXUS	N/A	CBP	Highway
Secure Electronic Network for Travelers Rapid Inspection	SENTRI	CBP	Highway
U.S. Passport	N/A	U.S. State Department	All
RAPIDGate	N/A	Eid Passport, Inc.	Highway
Common Access Card	CAC	Department of Defense	Highway

been fully implemented.(*12,13*) The legislative authority for both began in 2002 with the MTSA and continued with the Security and Accountability for Every Port Act of 2006 (SAFE Port Act).

The timeline provides a visual representation of not only the time frame within which these credentials were developed and implemented, but also a reflection of their functionality and changes to the security and communication environments. Prior to 1995, the majority of credentials were designed to ensure that the credential-holder possessed the necessary capabilities (e.g., MML, STCW, and CDL). The drastic increase in the number of credentials after 1995 reflects, at least in some part, the technological advances of communication (e.g., the Internet), data collection techniques (e.g., online applications, digital photographs, digital fingerprints, etc.), and data storage capabilities (e.g., database structures, encryption software,

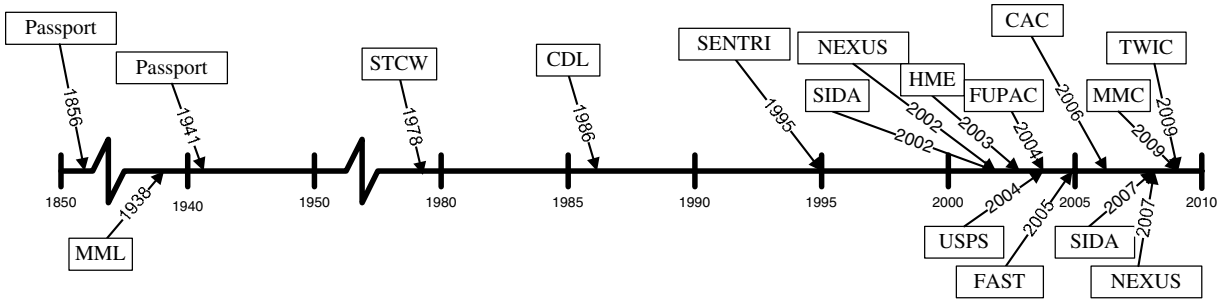

Figure 3-1. Credential timeline.

and secure network connections). The number of credentials developed since 2002 is, to some extent, the result of the flurry of legislation resulting from the terrorist attacks of September 11, 2001. Security credentials became the regulatory method of effecting access control.

Credential Categorization

Credentials were then categorized based on their primary purpose of security (i.e., confirms that a person does not pose a security threat, establishes that a person possesses lawful status in the United States, and verifies identity) or safety (i.e., verifies a person's "skill" qualifications). Figure 3-2 illustrates this segregation of the credentials into the categories of security or safety. Of these credentials, 13 were designed primarily to function as a security authentication for the credential-holder, 4 were designed primarily to certify the skill qualifications of the credential-holder (i.e., the MML, STCW, Pilot's License, and Engineer's License), and 2 function as both a means of security and safety (i.e., the CDL-HME and MMC). The HazMat endorsement for the CDL requires a threat assessment (*14*), thus vetting the credential-holder from a security perspective. The MMC is a consolidation of the MMD, MML, and STCW.(*12*) It requires both a demonstration of the abilities of the credential-holder (MML and STCW) and a determination of the perceived security risk (MMD) of the credential-holder.

This research effort was tasked with evaluating security credentials for persons who transport hazardous materials. As such, those credentials without a primary purpose of vetting the credential-holder and communicating the information necessary to determine the credential-holder's validity were dropped from the remaining analysis efforts. These safety credentials were simply outside the scope of this project.

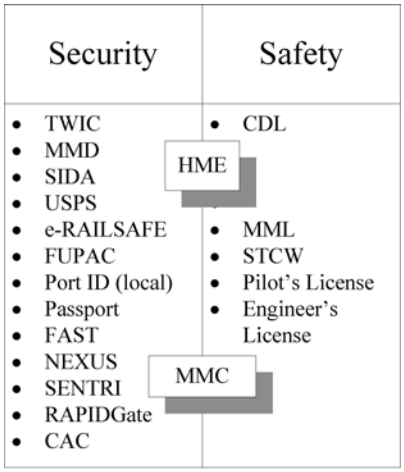

Figure 3-2. Credential categorization.

Requirements-to-Obtain Elements

During the application process, the issuing agencies require those seeking to obtain a security credential to submit various types of information (e.g., name, address, Social Security Number). These requirements to obtain were gathered through the individual applications and organized into several matrices to illustrate overlap or uniqueness among the various security credentials. These matrices were grouped by transportation mode to aid in identifying common requirements. Due to the number of identified requirements to obtain, the results were split into two matrices. Table 3-2 illustrates all requirements to obtain that apply to more than one credential. There are 34 singularly applicable requirements to obtain (that is, applicable to only one credential) that are tabulated in Appendix B.

There are 30 requirements to obtain that apply to more than one credential. An applicant must submit his or her full name, date of birth, citizenship information, address, and undergo a security threat assessment for all of the identified security credentials. Additionally, two of the requirements are applicable to 91% of the identified credentials: place of birth (not applicable to the CDL-HME) and fingerprinting (not applicable to the passport). In total, 16 requirements apply to the majority (>50%) of the identified credentials, including the 9 requirements previously listed: sex (82% applicable), Social Security Number (73% applicable), phone number (64% applicable), aliases (64% applicable), height (55% applicable), eye color (55% applicable), hair color (55% applicable), employer name (55% applicable), and e-mail address (55% applicable). In total, there are 64 different requirements of an applicant to obtain each of the 11 identified security credentials. Only 25% of the requirements apply to the majority (>50%) of credentials, and only 8% of the requirements are universally applicable across all 11 identified credentials.

Table 3-3 groups all background-check processes into the security threat assessment category. This was done to simplify the table for comparison purposes. However, this is an important aspect of the security credentials, especially with regard to duplication of effort and redundant costs (refer to the cost analysis section). Table 3-3 specifies the background check processes for each credential.

The fingerprint-based criminal records check refers to the background check performed by the Federal Bureau of Investigation (FBI) using the National Crime Information Center (NCIC). Regardless of the issuing agency, the FBI performs this portion of the investigation and then provides the relevant data to the issuing agency (or adjudicating organization). A name-based investigation of relevant databases includes non-fingerprint criminal history record checks (e.g., U.S. passport), and a review of the Terror Watch List (e.g., TWIC, MMC, and HME) maintained by DHS. This could also include other databases as the issuing agency may deem fit for a given circumstance. The MMD requires a drug test as part of the application

Table 3-2. Requirements to obtain credential.

Credential	Applicable Mode	Full Name	Date of Birth	Citizenship Information	Address	Security Threat Assessment	Place of Birth	Fingerprinting	Sex	Social Security Number	Phone Number	Aliases	Height	Eye Color	Hair Color	Employer's Name	Weight	Email Address	Employer's Address	Occupation	Address History	Employer's Phone Number	Employment History	Vision Test	National Drivers Registry Check	Fax Number	Next of Kin	Character References	Hearing Test	Medical or Physical Exam	Nickname
SIDA	Air	●	●	●	●	●	●	●	●	●		●	●	●	●	●	●		●												
Passport	All	●	●	●	●	●	●		●	●	●	●	●	●	●	●		●		●											
TWIC	Marine	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●		●				●					
MMD	Marine	●	●	●	●	●	●	●		●	●		●	●	●		●	●						●	●	●	●	●	●	●	
MMC	Marine	●	●	●	●	●	●	●		●	●		●	●	●		●	●						●	●		●	●	●	●	
CDL-HME	Highway	●	●	●	●	●		●	●	●	●		●	●	●		●							●							
FAST	Highway	●	●	●	●	●	●	●	●			●				●			●	●	●	●	●								●
USPS	Highway	●	●	●	●	●	●	●	●	●	●	●				●			●		●	●	●								
NEXUS	Highway	●	●	●	●	●	●	●	●		●	●				●		●	●	●	●	●	●								●
SENTRI	Highway	●	●	●	●	●	●	●	●			●									●		●								
CAC	Highway	●	●	●	●	●	●	●	●	●								●													

process, and results of the test are included in the adjudication process. A review of the National Driver Register is required for the MMD, MMC, and USPS credentials. In each case, one's driving record can influence the application process (refer to the disqualifying offenses section). Finally, an interview with issuing agency personnel is required for the three CBP-issued credentials (FAST, NEXUS, and SENTRI).

It is important to note that the agencies performing the background checks remain relatively consistent; for instance, the FBI is responsible for the criminal history records checks for each of the credentials (name- and fingerprint-based). For each credential requiring a review of the Terror Watch List, as stated, there is only one clearinghouse for this information via the FBI. The key difference for many of the credentials is the process of adjudication. Each issuing agency receives the results of all background check processes and determines the applicant's eligibility for the credential.

Attribute Elements

Once the credential is obtained, there are distinctive attributes on, or within, each credential that are used by both security personnel and others to authenticate the identity and intentions of the credential-holder. These attributes were gathered by examining actual photo renderings, or textual descriptions, of credentials. Table 3-4 lists those elements that are displayed on, or contained within, the credential. Where each attribute applies to a given credential there is a corresponding mark noting the relationship. This attribute matrix in Table 3-4 is grouped by transportation mode to provide a

Table 3-3. Credential background checks.

	TWIC	HME	MMD	MMC	SIDA	FAST	NEXUS	SENTRI	USPS	Passport	CAC
Fingerprint-Based Criminal Records Check	●	●	●	●	●	●	●	●	●		●
Name-Based Relevant Database Check	●	●	●	●	●	●	●	●		●	●
Drug Test			●	●							
National Driver Register Check			●	●					●		
Interview						●	●	●			

Table 3-4. Credential attributes matrix.

Credential	Applicable Mode	Full Name	Date of Expiration	Photograph	Tamper-resistant features	Unique Serial Number	Date of Birth	Citizenship	Sex	Endorsements	Bar Code	Signature	If found	Authorization Agency	Issuing Location/Branch	Radio Frequency Identification	Date of Issue	Address	Eye Color	Height	Employer	Place of Birth	Hair Color	Weight	Dual Interface ICC	Social Security Number	Magnetic Strip	Access Level
SIDA	Air	●	●	●	●	●				●	●		●	●			●				●						●	●
Passport	All	●	●	●	●	●	●	●	●	●		●		●		●	●					●						
TWIC	Marine	●	●	●	●																				●			
MMD	Marine	●	●	●	●	●	●	●		●		●		●	●			●	●	●			●	●		●		
MMC	Marine	●	●	●	●	●		●	●	●		●	●	●				●										
CDL-HME	Highway	●	●	●	●	●	●		●	●	●	●						●	●	●								
FAST	Highway	●	●	●	●	●	●	●	●		●		●			●			●	●		●	●	●				
USPS	Highway	●	●	●							●	●	●		●		●				●							
NEXUS	Highway	●	●	●	●	●	●	●	●		●		●		●	●	●											
SENTRI	Highway	●	●	●	●		●	●	●						●	●												
CAC	Highway	●	●	●	●		●			●	●			●							●				●	●	●	●

graphic representation of the similarities among credentials within a particular mode.

There are 27 unique attributes identified from 11 credentials. Three attributes, full name, date of expiration, and photograph, are common to all credentials. Ten of the attributes apply to the majority (>50%) of the credentials. In addition to the three previously stated, the other seven include: tamper-resistant features (91% applicable), unique serial number (64% applicable), date of birth (64% applicable), citizenship (55% applicable), sex (55% applicable), endorsements (55% applicable), and bar code (55% applicable).

Table 3-5 provides a brief overview of the technology types and associated information contained within the specified credentials. In some cases (e.g., TWIC), the credentials have been designed to allow for additional information to be stored on the credential.

Disqualifying Offenses

Disqualifying offenses are those offenses that would bar an applicant from qualifying for a credential. In many cases these are specific criminal violations that are stated as such. In some cases, the disqualifying offenses are related to monetary infractions, applicant flight risk, or suspicion of an applicant based on intelligence information. The disqualifying offenses are grouped by issuing agency rather than credential; this is to provide an understanding of the threats, or perceived threats, for each issuing agency. Again, a list of the issuing agencies can be found in Table 3-1 of this report.

TSA (*15–19*)

TWIC

- Permanent Disqualifying Criminal Offenses—no time limit
  - Espionage or conspiracy to commit espionage;
  - Sedition or conspiracy to commit sedition;
  - Treason or conspiracy to commit treason;
  - A crime listed in 18 U.S.C. Chapter 113B—Terrorism or conspiracy to commit such a crime;
  - A crime involving a transportation security incident;
  - Improper transportation of a hazardous material;
  - Unlawful possession, use, sale, distribution, manufacture, purchase, receipt, transfer, shipping, transporting, import, export, storage of or dealing in an explosive or explosive device;
  - Murder;
  - Threat or maliciously conveying false information knowing the same to be false, concerning the deliverance, placement, or detonation of an explosive or other lethal device in or against a place of public use, state or government facility, a public transportation system, or an infrastructure facility;
  - Certain Racketeer Influenced and Corrupt Organizations (RICO) Act violations (in which the predicate act is one of the permanently disqualifying crimes);
  - Conspiracy or attempt to commit crimes in 49 CFR Part 1572 Subpart B Paragraph (a)(5)—(a)(10);
- Interim Disqualifying Criminal Offenses—Conviction within 7 years, or release from incarceration within 5 years,

Table 3-5. Credential technology description.

Credential	Technology	Information
TWIC	Smart Card • Dual interface integrated circuit chip (ICC) • Magnetic strip • Bar code	Photograph Fingerprints Personal ID number Meets FIPS 201-1 & ANSI 322 Standards Durability tests performed: -Flexure -U/V exposure -Humidity -Surface abrasion -Fading -Laundry test
CDL-HME	3-D bar code	Name, address Endorsements, restrictions Birth date, expiration date ID number Sex, eye color, height There may be some variance due to issuing state.
SIDA	Magnetic strip 26-bit encryption. Different badge colors for levels of access. Embedded hologram.	Contains a 6-digit number defining levels of access.
FAST NEXUS SENTRI	An antenna and integrated-circuit radio frequency identification (RFID) containing a unique number to verify the identity of the bearer to border protection officers.	Unique serial number The number is read wirelessly and sent to back-end computer systems. The systems retrieve personally identifiable information. (The unique number does not in itself contain any personally identifiable information.) The systems involved are law enforcement databases, watch lists, and credential application information.
Passport	Embedded Electronic Chip (RFID)	New ePassports contain an embedded chip that is a duplicate electronic copy of all information from the data page—name, date of birth, place of birth, issuing office, and a digitized photo.

of application; includes wants and warrants associated with the following crimes:

– Unlawful possession, use, sale, manufacture, purchase, distribution, receipt, transfer, shipping, transporting, import, export, storage of or dealing in a firearm or other weapon;
– Extortion;
– Dishonesty, fraud, or misrepresentation, including identity fraud and money laundering;
– Bribery;
– Smuggling;
– Immigration violations;
– Distribution, possession with intent to distribute, or importation of a controlled substance;
– Arson;
– Kidnapping or hostage-taking;
– Rape or aggravated sexual abuse;
– Assault with intent to murder;
– Robbery;
– Lesser violations of the RICO Act; or
– Conspiracy or attempt to commit crimes in 49 CFR 1572 Subpart B Paragraph (b).

USCG (*20*)

MMC

Table 3-6 illustrates the disqualifying offenses for the MMC.

Individual States (*21–22*)

CDL-HME

The TSA performs the security threat assessment for HMEs; thus, it is the same for all states.

- Permanently Disqualifying Criminal Offenses—Applicants are permanently disqualified from holding an HME on a state-issued CDL if convicted or found not guilty by reason of insanity for any of the following crimes:

Table 3-6. Disqualifying offenses for the MMC.

Crime[1]	Minimum	Maximum
Assessment Periods for Officer and Rating Endorsements		
	Year(s)	**Years**
Crimes against Persons		
Homicide (intentional)	7	20
Homicide (unintentional)	5	10
Assault (aggravated)	5	10
Assault (simple)	1	5
Sexual assault (rape, child molestation)	5	10
Robbery	5	10
Other Crimes against Persons[2]		
Vehicular Crimes		
Conviction involving fatality	1	5
Reckless driving	1	2
Racing on the highways	1	2
Other vehicular crimes		
Crimes against Public Safety		
Destruction of property	5	10
Other crimes against public safety		
Dangerous Drug Offenses[3,4,5]		
Crime	**Minimum**	**Maximum**
Trafficking (sale, distribution, transfer)	5	10
Dangerous drugs (use or possession)	1	10
Other dangerous drug convictions[6]		
Assessment Periods for Officer Endorsements Only		
Criminal Violations of Environmental Laws		
Criminal violations of environmental laws involving improper handling of pollutants or HazMat	1	10
Crimes against Property		
Burglary	3	10
Larceny	3	5
Other crimes against property		

Notes:
[1]Convictions of attempts, solicitations, aiding and abetting, accessory after the fact, and conspiracies to commit criminal conduct listed in this table carry the same minimum and maximum assessment periods provided in the table.
[2]Other crimes will be reviewed by the USCG to determine the minimum and maximum assessment periods depending on the nature of the crime.
[3]Applicable to original applications only. Any applicant who has ever been the user of, or addicted to the use of, a dangerous drug shall meet the requirements of Paragraph (f) of 46 CFR §10.211. Note: Applicants for reissue of an MMC with a new expiration date, including a renewal or additional endorsement(s), who have been convicted of a dangerous drug offense while holding a license, MMC, MMD, STCW endorsement or Certificate of Registry (COR), may have their application withheld until appropriate action has been completed by the USCG under regulations that appear in 46 CFR Part 5 governing the administrative actions against merchant mariner credentials.
[4]The USCG may consider dangerous drug convictions more than 10 years old only if there has been another dangerous drug conviction within the past 10 years.
[5]Applicants must demonstrate rehabilitation under Paragraph (I) of this section [§10.211 (46 CFR)], including applicants with dangerous drug use convictions more than 10 years old.
[6]Other dangerous drug convictions will be reviewed by the USCG on a case-by-case basis to determine the appropriate assessment period depending on the nature of the offense.

- Espionage;*
- Sedition;*
- Treason;*
- A crime listed in 18 U.S.C. Chapter 113B—Terrorism, or a state law that is comparable;*
- Bomb threats;
- Crime involving a transportation security incident;
- Improper transportation of hazardous materials under 49 U.S.C. 5124 or a comparable state law;
- Unlawful possession, use, sale, distribution, manufacture, purchase, receipt, transfer, shipping, transporting, import, export, storage of or dealing in an explosive or explosive device;
- Murder;

*Not eligible for a waiver

  - Violations of the RICO Act under 18 U.S.C. 1961, or a comparable state law, where violations consist of any of the permanent disqualifying offenses; or
  - Conspiracy or attempt to commit any of these crimes.
- Interim Disqualifying Criminal Offenses—If convicted or found not guilty by reason of insanity within the previous 7 years, or released from prison in the last 5 years, for any of the following crimes:
  - Unlawful entry into a seaport;
  - Assault with intent to murder;
  - Kidnapping or hostage-taking;
  - Rape or aggravated sexual abuse;
  - Unlawful possession, use, sale, manufacture, purchase, distribution, receipt, transfer, shipping, transporting, delivery, import, export of or dealing in a firearm or other weapon;
  - Extortion;
  - Dishonesty, fraud, or misrepresentation, including identity fraud;
  - Bribery;
  - Smuggling;
  - Immigration violations;
  - Violations of the RICO Act under 18 U.S.C. 1961, or a comparable state law, other than any permanent disqualifying offenses;
  - Robbery;
  - Distribution of, intent to distribute, or importation of a controlled substance;
  - Arson; or
  - Conspiracy or attempt to commit any of these crimes.

CBP (*23–25*)

FAST, NEXUS, SENTRI

- Disqualifying Offenses
  - Provided false or incomplete information on the application;
  - Have been convicted of a criminal offense;
  - Have a criminal conviction for which applicant received a pardon;
  - Have failed to obtain a waiver of inadmissibility to the United States when applicable;
  - Have been found in violation of customs or immigration law;
  - Fail to meet other requirements of the FAST Commercial Driver Program;
  - Will not lawfully reside in either Canada or the United States for the term of their NEXUS membership;
  - Are inadmissible to the United States or Canada under applicable immigration laws;
  - Have pending criminal charges to include outstanding warrants;
  - Have been found in violation of any customs, immigration, or agriculture regulations or laws in any country;
  - Are subject of an ongoing investigation by any federal, state, or local law enforcement agency;
  - Are inadmissible to the United States under immigration regulation, including applicants with approved waivers of inadmissibility or parole documentation; or
  - Cannot satisfy the CBP of a low risk status or meet other program requirements.

Individual Airport Authorities (*26*)

SIDA

- Disqualifying Offenses
  - Forgery of certificates, false marking of aircraft, and other aircraft registration violations (49 U.S.C. 46306);
  - Interference with air navigation (49 U.S.C. 46308);
  - Improper transportation of a hazardous material (49 U.S.C. 46312);
  - Aircraft piracy (49 U.S.C. 46502);
  - Interference with flight crew members or flight attendants (49 U.S.C. 46504);
  - Commission of certain crimes aboard aircraft in flight (49 U.S.C. 46506);
  - Carrying a weapon or explosive aboard aircraft (49 U.S.C. 46505);
  - Conveying false information and threats (49 U.S.C. 46507);
  - Aircraft piracy outside the special aircraft jurisdiction of the U.S. (49 U.S.C. 46502[b]);
  - Lighting violations involving transporting controlled substances (49 U.S.C. 46315);
  - Unlawful entry into an aircraft or airport area that serves air carriers or foreign air carriers contrary to established security requirements (49 U.S.C. 46314);
  - Destruction of an aircraft or aircraft facility (18 U.S.C. 32);
  - Murder;
  - Assault with intent to murder;
  - Espionage;
  - Sedition;
  - Kidnapping or hostage-taking;
  - Treason;
  - Rape or aggravated sexual abuse;
  - Unlawful possession, use, sale, distribution, or manufacture of an explosive or weapon;
  - Extortion;
  - Armed or felony unarmed robbery;
  - Distribution of, or intent to distribute, a controlled substance;
  - Felony arson;
  - Felony involving a threat;
  - Felony involving

  - Willful destruction of property;
  - Importation or manufacture of a controlled substance;
  - Burglary;
  - Theft;
  - Dishonesty, fraud, or misrepresentation;
  - Possession or distribution of stolen property;
  - Aggravated assault;
  - Bribery; or
  - Illegal possession of a controlled substance punishable by a maximum term of imprisonment of more than one year;
- Violence at international airports (18 U.S.C. 37); or
- Conspiracy or attempt to commit any of the criminal acts listed herein.

U.S. Department of State (*27–28*)

U.S. Passport

- Disqualifying Offenses
  - The department may not issue a passport, except a passport for direct return to the United States, in any case in which the department determines or is informed by competent authority that
    - The applicant is in default on a loan received from the United States under 22 U.S.C. 2671(b)(2)(B) for the repatriation of the applicant and, where applicable, the applicant's spouse, minor child(ren), and/or other immediate family members, from a foreign country (see 22 U.S.C. 2671[d]); or
    - The applicant has been certified by the secretary of Health and Human Services as notified by a state agency under 42 U.S.C. 652(k) to be in arrears of child support in an amount determined by statute.
  - The department may refuse to issue a passport in any case in which the department determines or is informed by competent authority that
    - The applicant is the subject of an outstanding federal warrant of arrest for a felony, including a warrant issued under the Federal Fugitive Felon Act (18 U.S.C. 1073);
    - The applicant is subject to a criminal court order, condition of probation, or condition of parole, any of which forbids departure from the United States and the violation of which could result in the issuance of a federal warrant of arrest, including a warrant issued under the Federal Fugitive Felon Act;
    - The applicant is subject to a U.S. court order committing him or her to a mental institution;
    - The applicant has been legally declared incompetent by a court of competent jurisdiction in the United States;
    - The applicant is the subject of a request for extradition or provisional request for extradition that has been presented to the government of a foreign country;
    - The applicant is the subject of a subpoena received from the United States pursuant to 28 U.S.C. 1783, in a matter involving federal prosecution for, or grand jury investigation of, a felony;
    - The applicant is a minor and the passport may be denied under 22 CFR 51.28;
    - The applicant is subject to an order of restraint or apprehension issued by an appropriate officer of the U.S. Armed Forces pursuant to Chapter 47 of Title 10 of the U.S. Code;
    - The applicant is the subject of an outstanding state or local warrant of arrest for a felony; or
    - The applicant is the subject of a request for extradition or provisional arrest submitted to the United States by a foreign country.
  - The department may refuse to issue a passport in any case in which:
    - The applicant has not repaid a loan received from the United States under 22 U.S.C. 2670(j) for emergency medical attention, dietary supplements, and other emergency assistance, including, if applicable, assistance provided to his or her child(ren), spouse, and/or other immediate family members in a foreign country;
    - The applicant has not repaid a loan received from the United States under 22 U.S.C. 2671(b)(2)(B) or 22 U.S.C. 2671(b)(2)(A) for the repatriation or evacuation of the applicant and, if applicable, the applicant's child(ren), spouse, and/or other immediate family members from a foreign country to the United States;
    - The applicant has previously been denied a passport under this section or 22 CFR 51.61, or the department has revoked the applicant's passport or issued a limited passport for direct return to the United States under 22 CFR 51.62, and the applicant has not shown that there has been a change in circumstances since the denial, revocation, or issuance of a limited passport that warrants issuance of a passport; or
    - The secretary determines that the applicant's activities abroad are causing, or are likely to cause, serious damage to the national security or the foreign policy of the United States.
  - The department may refuse to issue a passport in a case in which the department is informed by an appropriate foreign government authority or international organization that the applicant is the subject of a warrant of arrest for a felony.
  - The department may refuse to issue a passport, except a passport for direct return to the United States, in any case in which the department determines or is informed by a

competent authority that the applicant is a minor who has been abducted, wrongfully removed or retained in violation of a court order or decree, and return to his or her home state or habitual residence is necessary to permit a court of competent jurisdiction to determine custody matters.

– A passport may not be issued in any case in which the department determines or is informed by a competent authority that the applicant is subject to imprisonment or supervised release as the result of a felony conviction for a federal or state drug offense if the individual used a U.S. passport or otherwise crossed an international border in committing the offense, including a felony conviction arising under
  - The Controlled Substances Act (21 U.S.C. 801 et seq.) or the Controlled Substances Import and Export Act (21 U.S.C. 951 et seq.);
  - Any federal law involving controlled substances as defined in section 802 of the Controlled Substances Act (21 U.S.C. 801 et seq.);
  - The Bank Secrecy Act (31 U.S.C. 5311 et seq.) or the Money Laundering Act (18 U.S.C. 1956 et seq.) if the department is in receipt of information that supports the determination that the violation involved is related to illicit production of, or trafficking in, a controlled substance; or
  - Any state law involving the manufacture, distribution, or possession of a controlled substance.
– A passport may be refused in any case in which the department determines or is informed by a competent authority that the applicant is subject to imprisonment or supervised release as the result of a misdemeanor conviction of a federal or state drug offense if the individual used a U.S. passport or otherwise crossed an international border in committing the offense, other than a first conviction for possession of a controlled substance, including a misdemeanor conviction arising under
  - The federal statutes described in §51.61(a); or
  - Any state law involving the manufacture, distribution, or possession of a controlled substance.
– Notwithstanding paragraph (a) of this section [22 CFR §51.61] the department may issue a passport when the competent authority confirms, or the department otherwise finds, that emergency circumstances or humanitarian reasons exist.

USPS (9)

Disqualifying Factors

- Subject of an outstanding warrant;
- Convicted of illegally using, possessing, selling, or transferring controlled substances within the last 5 years;
- Convicted of a felony criminal charge within the last 5 years;
- Convicted of offenses involving dishonesty, moral turpitude, financial gain, or assault within the past 5 years;
- On parole, probation, or under a suspended sentence for commission of a felony or any controlled substance charge;
- Pending felony charges or any pending controlled substance charge;
- Has an established pattern of criminal conduct that could undermine the efficiency of the Postal Service or safety of its employees; or
- Convicted of, under investigation for, or under indictment for stealing mail or other postal crimes.

Time and Cost Analyses

Time-to-Acquire Questionnaire Analyses

The consolidated questionnaire became active on a commercial hosting Web site (SurveyMonkey) on April 20, 2010. The questionnaire was promoted to credential-holders via communications with TAG members, industry groups, labor organizations, and word-of-mouth recruitment. Data collection lasted 10 weeks and is shown by respondents and mode in Figure 3-3. A total of 378 respondents completed the time-to-acquire questionnaire by June 30, 2010.

Sample Demographics

Respondents' demographic information was collected. The demographic data included the respondents' age, sex, experience transporting hazardous materials, role in the transportation process, transportation mode, and credentials. The majority of respondents (95.3%; 304 respondents) were male; only 4.7% (15 respondents) were female. Most of the respondents were 45 to 54 years old (41.1%; 131 respondents), 55 to 64 years old (31%; 99 respondents), or 35 to 44 years old (18.8%; 60 respondents). The youngest respondents were under 25 years old (0.3%; 1 respondent) and 25 to 34 years old (3.4%; 11 respondents). The oldest respondents were 65 to 74 years old (5.3%; 17 respondents). There were no respondents who reported they were 75 years or older. However, 59 respondents failed to provide sex or age data. Respondents also were asked how long they had been involved with the transportation of hazardous materials. Of the 317 respondents who answered this question, 12.9% (41 respondents) had less than 5 years' experience, 12.6% (40 respondents) had 5 to 9 years' experience, 12% (38 respondents) had 10 to 14 years' experience, 14.2% (45 respondents) had 15 to 19 years' experience, 15.5% (49 respondents) had 20 to 25 years' experience, and 32.8% (104 respondents) had over 25 years' experience.

Respondents self-reported their roles in the transportation process. Respondents were asked to provide the title that best

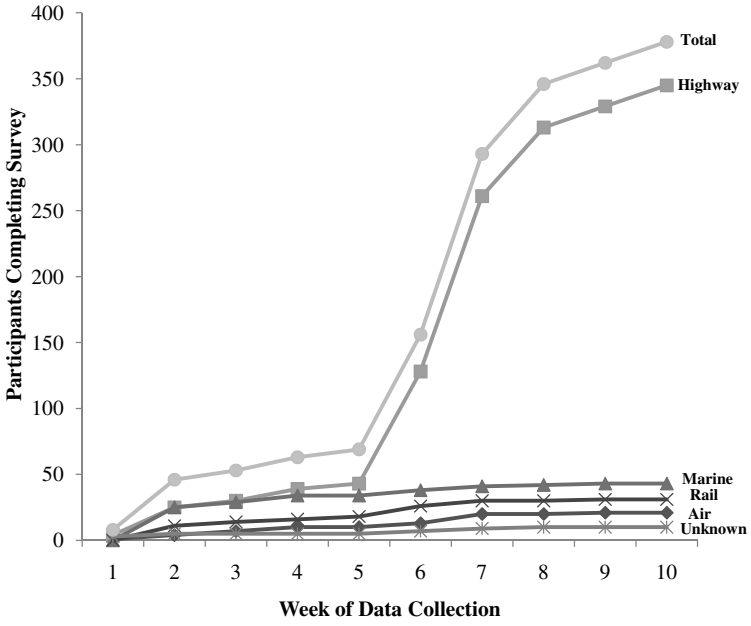

Figure 3-3. Data collection progress by mode.

described their role in the transportation of hazardous materials. Of the 378 respondents, 307 provided answers to this question. Responses represented a wide range of professions (business owners, commercial truck drivers, port police) and supervisory responsibility (line workers such as railroad engineers, administrators in charge of port operations and security). Figure 3-4 provides a summary of the categories of roles that respondents indicated they held.

Most respondents worked in the highway/tractor trailer mode (93.8%; 345 respondents). There were 12% (44 respondents) who worked in the marine mode, 8.4% (31 respondents) worked in the rail mode, and 5.7% (21 respondents) reported that they worked in the air mode. Please note that some respondents chose multiple modes, thus the totals sum to more than 100%.

Questionnaire respondents were asked to indicate whether they held a number of credentials. Of the 364 respondents (out of 378 total respondents) who answered this question, 88.7% (323 respondents) held a CDL-HME and 67.9% (247 respondents) held a TWIC. The FAST credential was held by 14.3% (52 respondents), and 14.8% (54 respondents) reported holding an "other" credential. Figure 3-5 provides a summary of the credentials held. Respondents were asked what other credentials were required for their jobs. Additionally, individuals were asked to provide feedback on the other credentials held. Figure 3-6 illustrates those credentials for which individuals provided additional feedback. Credentials also were examined by mode. Figures 3-7 through 3-10 provide a breakdown of credentials held by mode. The majority of highway/tractor-trailer respondents held a CDL-HME and/or the TWIC. This is expected based on the nature of those credentials. Likewise, marine respondents also held the FUPAC, MMC, MMD, and MML.

Total Time to Obtain Credentials

Figure 3-11 provides a summary of the total time respondents needed to obtain their credentials, from completion of the application process through physical receipt of the credential. The majority of respondents completed the application process and received their credential within 2 months (81.5%).

Respondents provided an assessment of the total time needed to complete the application process and receive their credentials. Almost 40% of respondents considered that the time needed to obtain the credential was adequate. However, a combined 59.3% believed that the process took too long (39.1%) or way too long (20.2%). Only six respondents (1%) believed that the process was too short (Figure 3-12). A crosstab of the number of respondents reporting too long, way too long, and times to obtain a credential can be found in Appendix D.

Time to Complete Application

Respondents were asked to provide an estimate of the amount of time it took to complete the application process (i.e., from the time they started the application to the time the application was provided to the credentialing agency). The majority of respondents (63.2%; 361 respondents) (Figure 3-13) completed and submitted the application in less than 2 hours. However, 8.1% (46 respondents) indicated that

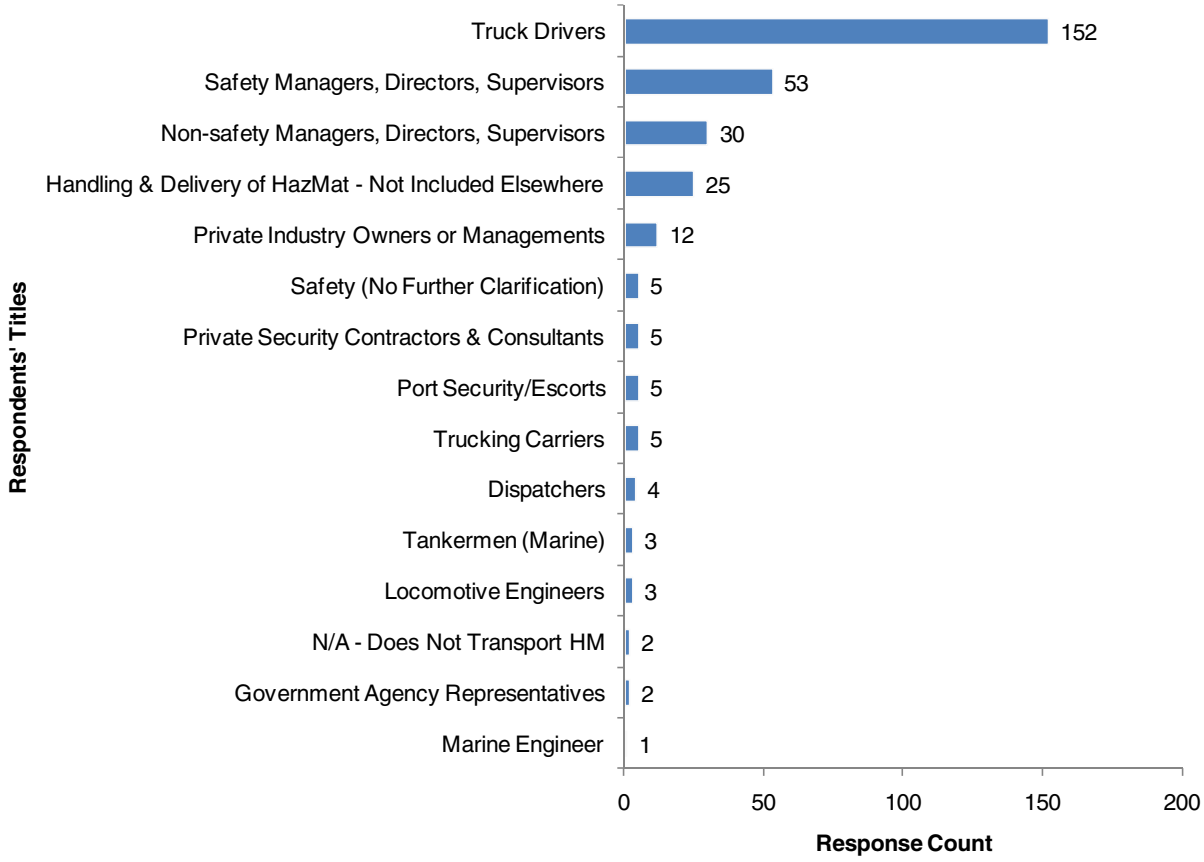

Figure 3-4. Administrators' roles in the transportation process.

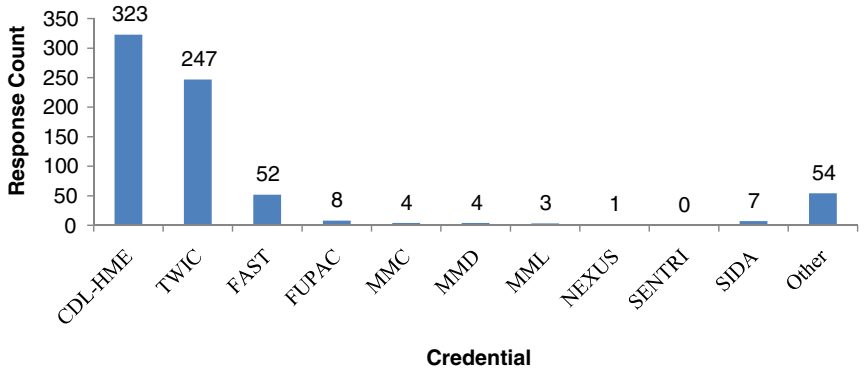

Figure 3-5. Credentials held by respondents.

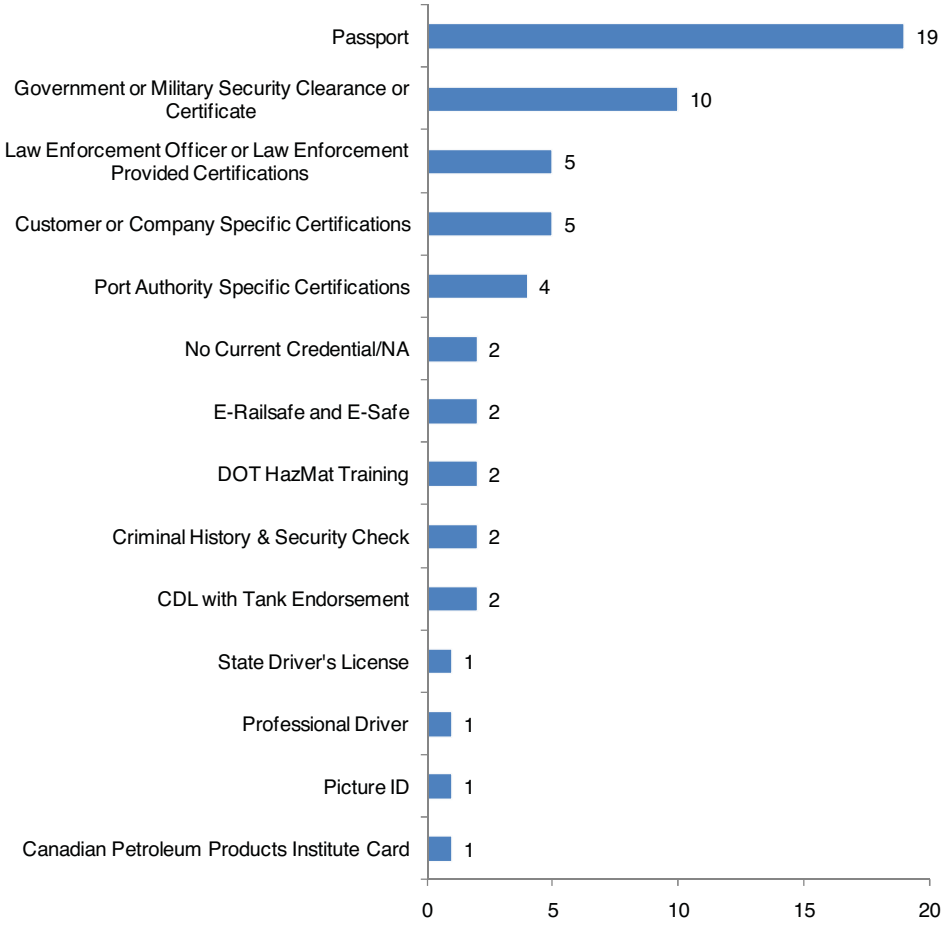

Figure 3-6. Other credentials for which respondents provided feedback.

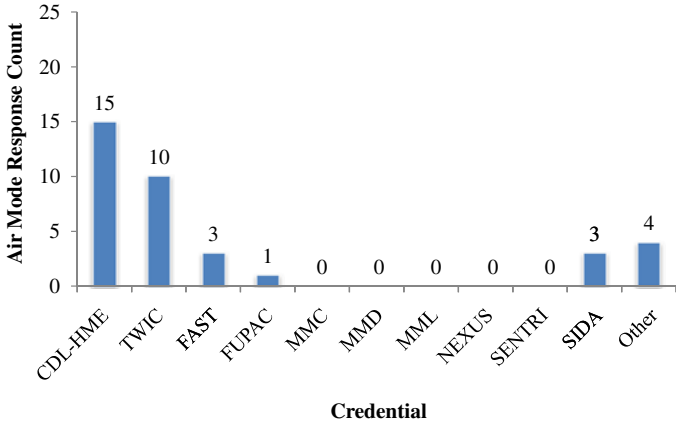

Figure 3-7. Credentials held by air mode respondents.

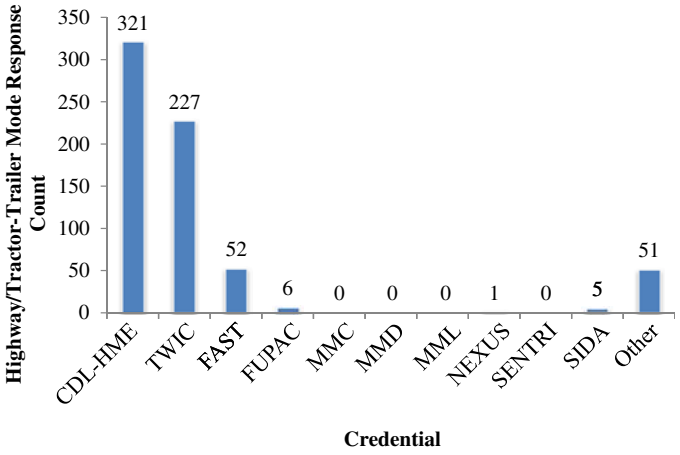

Figure 3-8. Credentials held by highway/ tractor-trailer respondents.

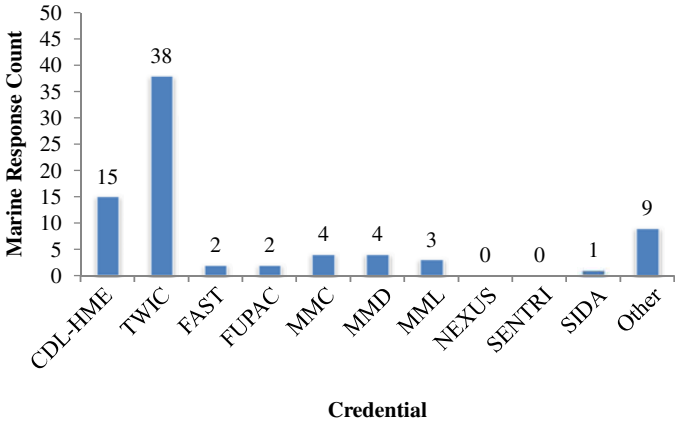

Figure 3-9. Credentials held by marine respondents.

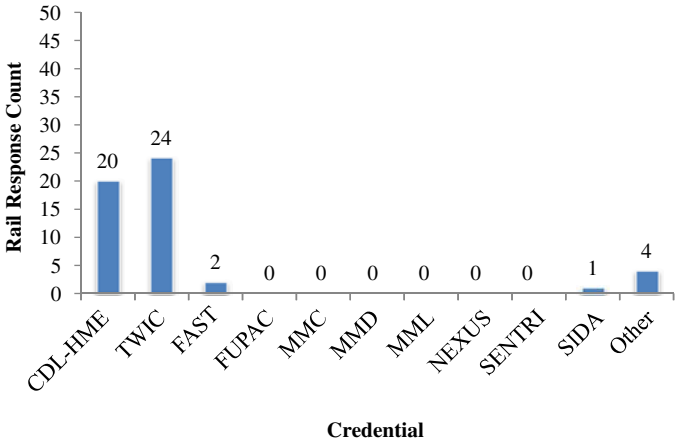

Figure 3-10. Credentials held by rail respondents.

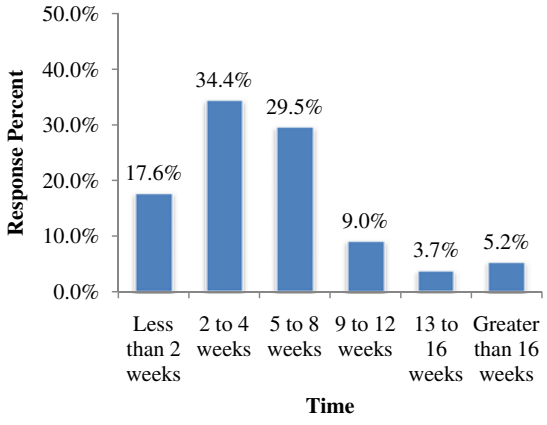

Figure 3-11. Summary of respondents' total time needed to obtain credentials.

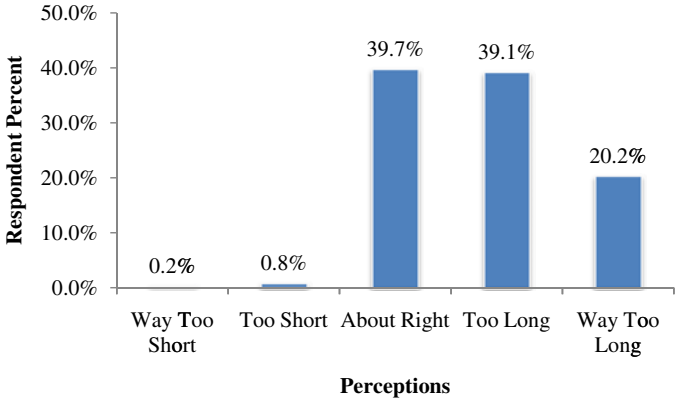

Figure 3-12. Respondents' perceptions regarding total time needed to obtain credential.

it took 5 or more hours to complete an application, with 1.2% (7 respondents) noting that the application took more than 16 hours to complete. Of those indicating that it took more than 16 hours to complete the application, three respondents were referring to the CDL, one was referring to the SIDA, one was referring to Department of Defense Security Clearance, one was referring to a training certificate, and one was referring to a terminal-specific access credential.

Respondents also reported their perceptions regarding the length of time it took for them to complete and submit their credential applications. As shown in Figure 3-14, most respondents (74.9%; 441 respondents) indicated that they believed the time needed to complete the application process was adequate. The remaining respondents thought that the application took too long (24.3%; 143 respondents) or way too long (6.3%; 37 respondents). Four respondents (0.7%) indicated that the process was too short. As stated, data linking respondent perception to reported time of application can be found in Appendix D.

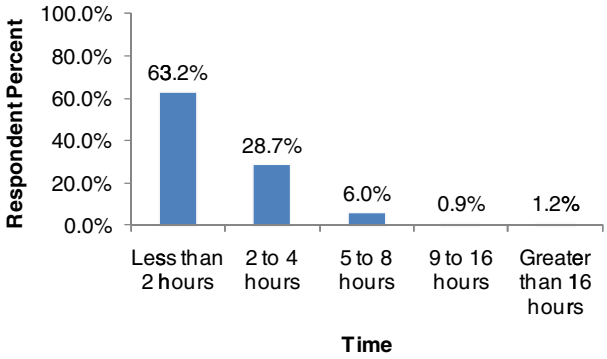

Figure 3-13. Summary of respondents' total time needed to complete the application process.

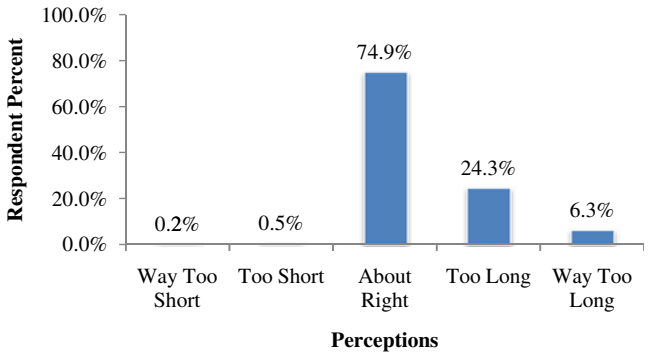

Figure 3-14. Respondents' perceptions regarding time needed to complete the application process.

Total Time to Pick Up Credentials

Due to concerns regarding the distance that applicants must travel to complete the credential application process, respondents were asked to provide an estimate of the total travel time needed to obtain their credentials once the credential was ready (Figure 3-15). The majority of respondents (75.1%; 441 respondents) traveled less than 2 hours to obtain their credentials. There were 92 respondents (15.7%) who traveled 2 to 4 hours, 33 respondents (5.6%) who traveled 5 to 8 hours, and 7 respondents (1.2%) who traveled 9 to 16 hours. Of the 2.4% (14 respondents) who indicated that they traveled more than 16 hours to obtain their credentials, they were referring to the following credential types:

- CDL-HME (1 respondent);
- TWIC (2 respondents);
- FAST (2 respondents);
- FUPAC (1 respondent);
- Other (8 respondents), which includes
  - DOT physical long form and the DOT vision waiver (1 respondent),
  - Government clearance (1 respondent),
  - Passport (2 respondents),
  - State-specific railroad commission credential (1 respondent),
  - e-RAILSAFE system badge (1 respondent),
  - Criminal history check (1 respondent), and
  - Non-specified (1 respondent).

Perceptions of the travel time required also were explored (Figure 3-16). The majority (64.4%; 378 respondents) indicated that the time needed to complete the application process was adequate. Less than 1% believed that the travel time was way too short or too short (0.5%, 3 respondents; and 0.3%; 2 respondents, respectively). The remaining 204 respondents (34.7%) indicated that they felt the travel time needed to pick up the credential took too long (26.7%; 157 respondents) or way too long (8.0%, 47 respondents). A full breakdown of perceptions corresponding with reported times are tabulated and graphically represented in Appendix D.

Additional Respondent Feedback

Respondents were provided an opportunity to express additional feedback regarding each credential they held. The CDL-HME feedback largely reflected redundancy concerns regarding the duplication of fees, security clearances, and fingerprinting. Respondents questioned the need for multiple credentials that relied on the same background check. Additionally, there was an inconvenience associated with completing the fingerprinting aspect of the application because applicants had to travel to get their fingerprints taken as

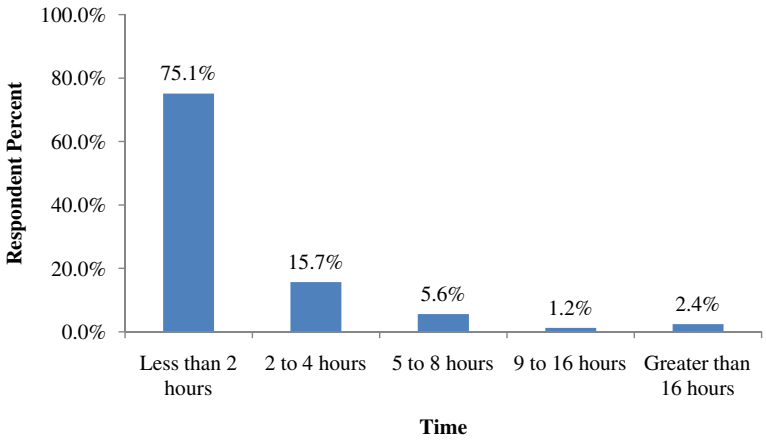

Figure 3-15. Summary of respondents' travel time needed to pick up credential.

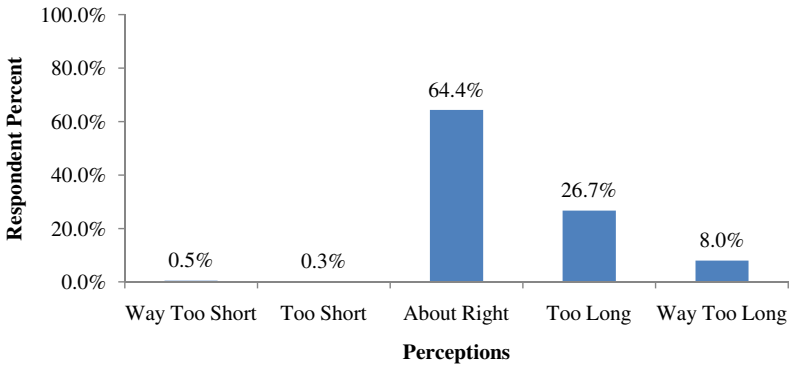

Figure 3-16. Respondents' perceptions regarding travel time needed to pick up the credential.

opposed to having them taken at a local facility. Specific comments included the following:

- "I pay a large fee to [state name redacted] for my CDL-HME, and then if I want to go into many of the ports I have to pay for a TWIC—which has the same background check—and then for a port issued credential as well—same background check."
- "Why so many background checks? Can't these agencies talk to one another? Who gets the money? Why $83 for one check and $132 for TWIC and $25 for TSA? Why isn't one background check enough?"
- "You have to go to [a] special place to get fingerprints done rather than [a] local law enforcement office. Our place is about 1.5 hours away which is not very efficient."
- "Had to travel 4 hours to do fingerprinting."

Respondents were equally vocal when it came to providing feedback for the TWIC. A large number of comments addressed the implementation and administration of this credential. Respondents voiced concerns associated with TWIC office administration and locations, the design of the cards and included technologies, and general redundancies that they saw between the TWIC and CDL-HME. Specific concerns were categorized as administrative, implementation, redundancy, and improper education. Representative comments are as follows:

- Administration Concerns
  - "TWIC offices were poorly administered. Too many losses of credential between offices."
  - "Was told TWIC was in, went to get it twice and computers were down."
  - "Need more TWIC Centers throughout the state."
  - "Why so expensive? The office had no parking for large trucks. Drivers had to take days off to get the TWIC."
- Implementation Concerns
  - "The readers should have been ready with the cards. As a 'flash' pass system it is a sham."
  - "The physical cards are too fragile. Not all of the technologies used in the card were properly tested and vetted. The failure rate of the actual cards is too high and there is a lack of understanding of the technologies used within the cards by the Trusted Agents involved in issuing the TWIC cards."
  - "The idea is good; the implementation is sketchy at best and the card is not being utilized to its fullest."
- Redundancy Concerns
  - "Too expensive especially because I already have a CDL with HME."
  - "TWIC is redundant having CDL-HME."
  - "How many background checks do I need to have?"
  - ". . . Again, why so many checks? If the different agencies can't talk to one another, what good is the system? $132 is a lot of money. This is another policy that only hurts the honest driver."
  - "The TWIC card was easy to get however because I hold a Hazmat endorsement it is redundant in my mind. These two should work together."
- Concerns resulting from a lack of or improper education
  - "Gotta wonder why we are really doing this."
  - "The applicant applying for the TWIC credential fails to understand the importance of providing proof of citizenship upon enrolling."

FAST respondents also voiced redundancy concerns. Again, a respondent expressed that s/he believed the credential to be a "waste of time and money." Respondents also articulated administration-related comments, including:

- "They lost it the first time."
- "There was some confusion about who I was because of someone with my same name that was a felon and it took a while to get the error corrected."

FAST respondents were also asked for their FAST credential designations. The majority, 65.2% (15 respondents), held North designations, while 8.7% (2 respondents) held South

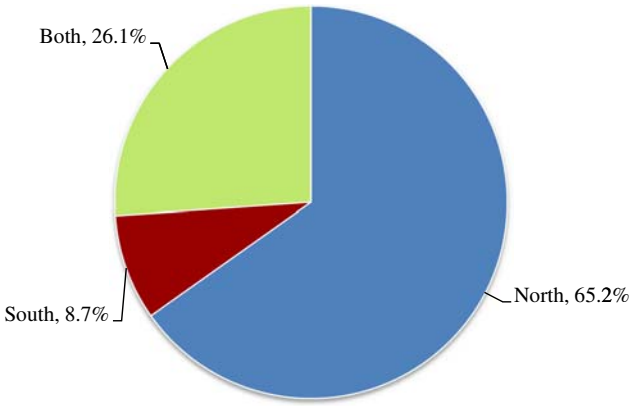

Figure 3-17. FAST credential designations.

designations. Additionally, 26.1% (6 respondents) held both North and South designations (Figure 3-17).

Three respondents who indicated they held a FUPAC provided feedback. Again, concerns focused on the redundancies seen within the system. Comments regarding the FUPAC are as follows:

- "Redundant gouging of my hard-earned dollars to do what my TWIC and CDL-HME already do. Clearly a cash cow for the port authority and nothing else."
- "[State name redacted] port's background checks are unnecessary, redundant, expensive, and time consuming."
- "Why did I have to get this thing[? I] already have a CDL [with] HME; for that matter why did I have to get the TWIC when I ALREADY HAVE A CDL [with] HME????? Does anyone realize what this is costing the drivers?"

In regard to the MMC, respondents only provided clarification as to the process for obtaining the credential. Both comments indicated that no travel time was required to obtain the credential, which was delivered via mail to a home address. The same comment was made for the MMD. However, it also was noted that the MMD should not be required since the MMC is in place. The comment associated with the SIDA simply indicated the agency affiliation of the respondent.

When provided an opportunity to comment on additional credentials, redundancy was again the focus. Feedback provided by respondents included the following:

- "Testing required every 2 years, same test over and over."
- "It's not about getting the credential as much as it is about duplicative efforts and one agency in the same department not [accepting] the information from another in the same department. Not just security issues either, i.e., physicals are a prime example—FAA, FMCSA, and USCG, to my knowledge, [none] of them [accept] this other at any level. [This causes] many in [state name redacted] heartburn."

Cost Analysis

The cost data were primarily collected through the online application process of the issuing agency. Many of the credentials had a specific cost stated on the agency Web site. The credentials, costs, and other associated data for 10 of the identified credentials are shown in Table 3-7.

The costs associated with each credential were limited to the monetary requirement to obtain the credential. In some cases, additional costs existed for various purposes, including replacement fees or varied rates for qualifying applicants. For instance, the cost to acquire a TWIC can be reduced if the applicant already possesses several qualifying credentials that required a security threat assessment. Should an applicant exercise that option, the expiration date will be 5 years from the issue date of the qualifying credential, rather than 5 years from the issuance of the TWIC. The cost of the SIDA badges is variable, and according to the issuing airport. The USPS credential cost is determined by contract with the supplier company, not the individual. Because of these factors, cost data are difficult to report. As part of the cost data collection effort, the research team included the time period that the credential was valid. Most credentials are valid for 5 years. The passport and CDL both last 10 years before renewal is required (assuming the credential-holder is 16 years or older for the passport). However, the HME portion of the CDL-HME must be renewed every 5 years, regardless of CDL renewal.

Since each state (and the District of Columbia) issues a separate CDL-HME credential, the research team placed the cost data in a separate cost table. Table E-1 (see Appendix E) includes both the costs of a new CDL credential with an HME endorsement as well as the costs for the threat assessment application for each state (and the District of Columbia). The credential fees for a CDL-HME (including threat assessment fees) ranged from a low of $107.25 (North Dakota) to a high of $326.25 (New York). Figure 3-18 provides the CDL count by cost range (excluding the cost for a threat assessment) for all 50 states and the District of Columbia.

Table 3-7. Credential costs.

Credential	Stated Costs	Valid for (Years)
SIDA	$91.33*	2
Passport	$100.00	10
TWIC	$132.50	5
MMD	$100.00	5
MMC	$100.00	5
FAST	$50.00	5
USPS	Unavailable	4
NEXUS	$50.00	5
SENTRI	$122.25	5
CAC	Unavailable	3

*SIDA costs are an arithmetic mean, see Appendix F.

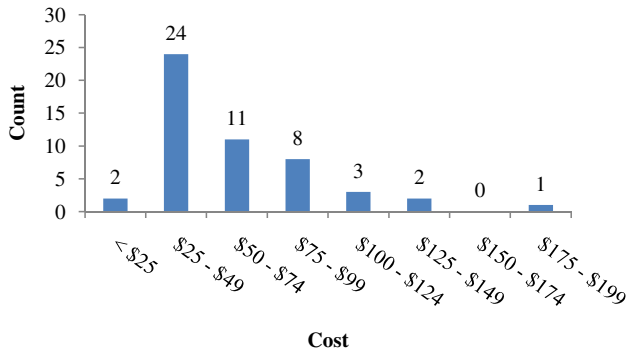

Figure 3-18. Counts by CDL Cost Range.

Although the majority of states charge between $25 and $50 for the CDL and HazMat endorsement, there is some amount of variation throughout the country. This appears to be due to variation in how each state structures its fees for licensing. In some cases the fee is mandated by state statute and thus a change to the fee requires legislative action. An increase in this fee may be politically untenable for state politicians. In other states the fee structure is required to reflect the cost to the state, and as such must continuously increase as the cost to the state increases. Federally mandated security threat assessment fees are shown in Figure 3-19.

When compared to the cost for the CDL, the variation is certainly less. This is most likely due to the fee structure originally set at the federal level. The few instances that vary are likely due to states that opted out of having the TSA collect the required data, and potentially are the result of additional processing at the issuing agency's prerogative.

Nine of the eleven identified credentials under consideration required fingerprinting to acquire. Thus, at least some of the costs associated with each credential cover the fingerprinting fee. Additionally, the requirements for criminal history record checks, criminal background checks, or security threat assessments for each of the credentials contribute to the total cost of the credential.

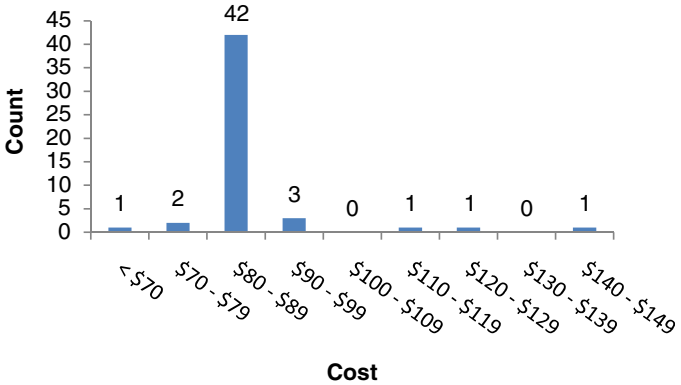

Figure 3-19. Counts by threat assessment cost range.

Use Cases

To better understand the user costs of credentialing, an additional cost analysis was conducted with self-reported costs of specific HazMat transportation workers. The use cases are drawn from the Web-based survey and telephone interviews with credential-holders. The use cases served two purposes. First, they identified the most commonly held combinations of credentials as identified by Web survey respondents and associated costs. Second, through interviews with current CMV drivers, out-of-pocket costs and time-to-obtain costs were explored.

Commonly held credentials were identified based upon a review of the HazMat Security Credential Survey responses. Survey respondents were asked if they currently held the following credentials: CDL-HME, TWIC, FAST, FUPAC, MMC, MMD, MML, NEXUS, SENTRI, SIDA, and other. Respondents' answers revealed 55 combinations of credentials. Due to the "other" option, 43 of the identified combinations were associated with only one respondent each. Looking at the 12 most common credentials, with input from the 43 other combinations, 5 combinations of credentials were chosen for further analysis. The combinations were chosen because they reflect the most commonly held credential combinations as well as combinations that would provide a multimodal perspective. Applying cost data to the most commonly held credentials provides a snapshot of the costs incurred by survey respondents (Table 3-8). The combined costs range from $232.50 to $434.72.

Five individuals were identified for follow-up interviews. The five individuals represented the highway/tractor-trailer mode and were CMV drivers. Four individuals were male and one was female. Mean years of experience was 20.7 years, with the median years of experience being 21.5 years. The mean age of responders was 56 and the median age was 58. The mean salary was approximately $53,000, which converts to an average hourly wage of $25.50. Four of the individuals spoken to held CDL-HME, TWIC, and U.S. passport credentials. One individual held a CDL-HME, a TWIC, and a credential issued by a local authority.

All interviewees held CDL-HMEs. The time it took them to obtain the CDL-HME ranged from 1 hour to 3 or 4 months. Four responded that it took 20 to 30 minutes to complete the application. One responded that it took all day, but that included the testing portion of the application as well. On average, the CDL-HME cost $100, for which only one received reimbursement. Although the application process was reported to be quick and fairly simple (especially if all data were gathered prior to completing the form), the cost and time associated with fingerprinting were noted. For example, one respondent has had his fingerprints taken four times, which required a 300-mile round trip each time.

Table 3-8. Cost information for the five most common credential combinations.

Credential Combination	Individual Credential Costs	Total Credential Combination Costs
CDL-HME and TWIC	$152.22[a] + $132.50	$284.72
CDL-HME, TWIC, and FAST	$152.22[a] + $132.50 + $50	$334.72
CDL-HME, TWIC, FAST, and U.S. Passport	$152.22[a] + $132.50 + $50 + $100	$434.72
CDL-HME, TWIC, and SIDA	$152.22[a] + $132.50 + $91.33[b]	$376.05
TWIC and MMC	$132.50 + $100.00	$232.50

Notes:
[a]Represents the mean combined CDL-HME stated cost ($61.96) and threat assessment fee ($90.26).
[b]Represents an average of identified SIDA fees (see Appendix F.)

All interviewees also held TWIC cards. The total time to obtain the TWIC ranged from 2 to 6 weeks and, on average, individuals spent 30 minutes completing the application. Three of the respondents indicated that they traveled 15 to 20 minutes to pick up their TWIC cards; however, one individual reported a shorter time and one noted that it was a 2-hour trip each way. On average, individuals paid $168 for the TWIC, a cost which all reported as being reimbursed. Additionally, individuals noted concern with the cost of renewing a credential, the duration of validity for a credential (especially for drivers with clean driving records), and that individuals should not wait until the last minute to apply.

Four of the interviewees noted that they held U.S. passports. On average, it took 3 weeks for the passport to arrive with the application completion time being, on average, 30 minutes. Only one individual traveled to pick up the passport while the others had the passports mailed to their homes. The average cost of the passport was $101.25 and all indicated that they were reimbursed this cost.

One individual held a credential that was issued by a local authority (in this case, a police department). The credential required an application, a background check, and a $200 fee, which the company did not reimburse. The total time to obtain the credential was 2 to 3 days. The time to complete the application was negligible (i.e., "quick") and required 15 miles travel to the police station to pick up the credential. Comments regarding this credential were similar to the comments made regarding this same credential in the Web-based survey. The purpose of this credential is perceived as being a revenue tool for the local authority versus a means of ensuring safety or security.

Based on the information above, the shortest amount of time it took to complete an application was 15 minutes and the longest it took to complete the application was 1 day. Using an hourly wage of $25.50 (assuming a working year of 2,080 hours), the shortest amount of lost work time due to completing the application converts to a loss of $6.38 in pay, while the longest amount of lost work time due to completing the application equals a loss of $255.50 in pay. However, none of the individuals indicated that they lost a day's work to obtain the credential. All noted that they obtained their credentials on personal time.

Assuming the minimum credential, application, and travel costs incurred by the individuals interviewed and their companies, the minimum average cost ranges from $375.63 (CDL-HME, TWIC, U.S. passport) to $468.00 (CDL-HME, TWIC, local authority credential). Conversely, assuming the maximum credential, application, and travel costs incurred by the individuals interviewed and their companies, the maximum average cost ranges from $726.75 (CDL-HME, TWIC, U.S. passport) to $825.50 (CDL-HME, TWIC, local authority credential).

Regulatory Analysis

The events of September 11, 2001, brought about renewed concerns regarding security and safety in the transport of hazardous materials across all modes. In response, Homeland Security Presidential Directive 12 (HSPD 12), dated August 27, 2004, "Policy for a Common Identification Standard for Federal Employees and Contractors," was implemented. HSPD 12 called for a single federal employee ID card. For all transportation modes, the principal policy objectives that supported the issuance of HazMat credentials were

- To ensure the trustworthiness of the passengers and the cargo flowing through the system;
- To ensure the trustworthiness of the transportation workers who operate and service the vehicles, assist the passengers, or handle the cargo;
- To ensure the trustworthiness of the private companies that operate in the system, such as the carriers, shippers, agents, and brokers; and,
- To establish a perimeter of security around transportation facilities and vehicles in operation.

Additionally, the USA PATRIOT Act of 2001 (Pub. L. 107-56) strengthened security for homeland defense against terrorism purposes. Of interest to this analysis is Section 1012 of Pub. L. 107-56, which places increased limitations on the

issuance of HazMat licenses. Section 1012 amends Chapter 51 of Title 49, U.S.C., by inserting a new section after Section 5103 (i.e., Section 5103a, *Limitation on Issuance of HazMat Licenses)*. Under Section 5103a, states may not issue or renew a license to operate a motor vehicle transporting hazardous materials in commerce unless the Secretary of Transportation has first determined through the receipt of a notification of results of a background check that the individual does not pose a security risk warranting denial of the license. The background check required under Section 5103a(c) is to be carried out by the Attorney General at the request of the state. The Attorney General is to complete a background check to include

- A check of the relevant criminal history databases;
- In the case of a foreign national, a check of the relevant databases to determine the status of the foreign national under the immigration laws of the United States; and
- As appropriate, a check of the relevant international databases through INTERPOL-U.S. National Central Bureau or other appropriate means.

As part of this analysis effort, upper-level security personnel in a number of the nation's ports were contacted. The purpose of this contact was to obtain expert insight into the acceptance of the TWIC as an authoritative security credential. Determining the acceptance of, and reliance upon, the TWIC by major ports was necessary because the regulations currently allow plant or facility owners to issue facility-specific identification cards as their access control measure, as long as it is ensured that individuals without a TWIC cannot gain unescorted access to secure areas and if the TWIC is checked at least once before the specific card is reissued or accepted. Of the 75 ports contacted, 35 continued to issue and require facility-specific security credentials. Forty of the ports contacted reported using only the TWIC as the authorized security access credential. Several ports that required only the TWIC noted that the requirement of an additional facility-specific identification would result in the duplication of federal security efforts. Appendix G contains the specific ports contacted and their corresponding responses.

Authorities, Policies, Programs, and Exemptions by Credential

To determine the feasibility of a consolidated security credential, one must consider the purpose each individual credential is intended to serve and its unique characteristics. Table 3-9 will provide an overview of the following features of each credential:

- **Authority:** Provides the authority under which the oversight agency created the security credential. The sources of authority discussed are
  - Congressional authority—The impetus for particular policies and/or the oversight organization itself is the result of legislative action;
  - Executive authority—Indicates the impetus originated with an executive order, executive directive, or agential rulemaking; and
  - Local authority—Refers to those policies established by state, local, or regional special authority (for example, the establishment of a port authority and subsequent port operating procedures).
- **Policy:** Outlines the desired outcome or effect of the action as well as guidelines that govern how laws or regulations should be put into operation.
- **Program:** Discusses the parties and organizations responsible for implementation of the policy and any specific requirements or modifications required for implementation, oversight, and governance.
- **Exemptions:** Presents any identified qualifiers to the aforementioned policies.

SWOT Analysis

Consolidated Credential Approach

The research team analyzed the feasibility of a consolidated credential using a SWOT analysis. The SWOT analysis for this project consisted of determining a proposed consolidation process, which was subsequently analyzed from two perspectives: security and cost-effectiveness.

Prior to analyzing the consolidation process, an explanation of the developed credentialing model will be provided, including the assumptions taken during analysis. For review of the identified credentials from Task 1, the research team identified not only the security credentials required of persons who transport hazardous materials but also the safety credentials that are related to the competency (or skill) of the person. The reasoning for this expanded analysis was twofold: (1) several credentials contained a mixture of security and safety components, and (2) it provided a complete depiction of the credentialing process.

Again, two of the identified credentials (CDL-HME and MMC) do not fit entirely into either security or safety, but overlap both categories. The CDL is a safety credential. To receive the HME endorsement one must demonstrate knowledge of HazMat shipping and regulatory procedures and undergo a security threat assessment per the USA PATRIOT Act. The MMC is a consolidation of the MMD, MML, and STCW. In each case, these credentials exhibit a dual intent and are, therefore, represented on a separate plane of the model indicating their uniqueness within the identified credentials (Figure 3-2).

Security involves two aspects: (1) the vetting process of the potential credential-holder, and (2) the capability to effectively

Table 3-9. Overview of credential by characteristic.

Transportation Worker Identification Credential (TWIC) (*29*)	
Authority	• Congressional
Policy	• Maritime Transportation Security Act of 2002, Public Law 107-295, Nov. 25, 2002, and 46 U.S.C. 70195 • The TWIC is used for visual identity checks. • It is anticipated that more than 1 million workers (*30*), including longshoremen, truckers, port employees, vessel crews, outer continental shelf facility workers, and all credentialed merchant mariners, will ultimately be covered by the TWIC.
Program	• TSA is required to issue a biometric, tamper-resistant security credential to individuals seeking unescorted access to port areas. • Initially it was intended to cover approximately 3,500 facilities, 10,800 vessels, and all USCG-credentialed merchant mariners.(*31*)
Exemption	• A TWIC applicant who has already secured an HME security threat assessment is not required to repeat the threat assessment in order to obtain the TWIC. • A non-TWIC holder may be escorted by a TWIC holder if the TWIC holder has met the security training requirements and has knowledge of escorting procedures and contingency plans if an escorted individual is engaged in another purpose aside from that for which they were granted access.
Commercial Driver's License—Hazardous Materials Endorsement (CDL-HME) (*32*)	
Authority	• Congressional • Executive
Policy	• The Commercial Motor Vehicle Safety Act of 1986, 49 USC 5103a, and 49 CFR 1572. • The CMVSA established minimum nationwide standards that must be met when a CDL is issued. Commercial drivers who carry hazardous materials must acquire a Class A, B, or C license and obtain an HME endorsement, which includes a HazMat knowledge test and a TSA HazMat Driver Threat Assessment, or an X endorsement, which is a combination of tank vehicle and HME endorsements. • 49 CFR 1572.9, the TSA HazMat Driver Threat Assessment Program, requires threat assessments for all individuals who apply for, renew, or transfer an HME onto their CDL.
Program	• States are to determine the application process, license fee, license renewal cycle, renewal procedures, and reinstatement requirements after a disqualification event. These processes and requirements must meet federal standards and criteria; however, states may exceed the federal requirements for certain criteria, such as medical, fitness, and other driver qualifications. • States must connect to the Commercial Driver's License Information System and the National Driver Register in order to exchange information about CDL drivers, traffic convictions, disqualifications, a driver's record, and to make certain that the applicant does not already have a CDL. • Applicants are required to pass a written test (consisting of 30 questions) pertaining to the over-the-road transport of hazardous materials, must comply with the standards specified in TSA requirements, and provide proof of citizenship or immigration status.
Exemption	• Each state must exempt individuals who operate CMVs for military purposes. • A state may, at its discretion, exempt firefighters, emergency response vehicle drivers, farmers, and drivers removing snow and ice in small communities • A state may issue a restricted license and waive the CDL knowledge and skills testing requirements for seasonal drivers in farm-related service industries and may waive certain knowledge and skills testing requirements for drivers in remote areas of Alaska. • A state also can waive the CDL-HME test requirements for part-time drivers working for the pyrotechnics industry.

(continued on next page)

Table 3-9. (Continued).

Merchant Mariner Document (MMD) (*33*)	
Authority	• Executive
Policy	• 33 CFR 101-106, 46 CFR Parts 10-16. • The MMD seeks to increase safety standards in the maritime industry with the goal of encouraging ongoing training and knowledge of advancements in the field, which is accomplished through the renewal process.
Program	• The U.S. Coast Guard's National Maritime Center oversees the issuance of the MMD. • The MMD was one of the standard documents required for all crewmembers of U.S. ships with a gross register tonnage (GRT) of more than 100 tons. • An entry-level MMD allowed a mariner to work on the deck as an Ordinary Seaman, in the Engine Department as a wiper, or in the Steward's Department as a food handler. With experience and testing, qualified ratings such as able seaman (AB) or qualified member of the Engine Department can be obtained. • All applicants for an MMD are required to take a drug test and undergo a criminal background check before receiving their documents, which may take anywhere from a few weeks to 6 months.
Exemption	• The MMD is being incorporated into the MMC. Mariners will receive the new credential when they apply for a new document or renew their current document. Current MMDs remain valid until their expiration date.
Merchant Mariner Credential (MMC) (*34*)	
Authority	• Executive
Policy	• 46 CFR Part 10 complies with the International Convention of the STCW, which was adopted by the International Maritime Organization in 1978 and amended in 1995. • The MMC is intended to be a single credential incorporating the MML, Certificate of Registry, STCW, and MMD as of April 15, 2009. • Much like the MMD, the MMC ensures ongoing training and knowledge of advancements in the field.
Program	• The U.S. Coast Guard's National Maritime Center oversees the issuance of the MMC. • The MMC has two categories, Domestic and International Endorsements. • The 14 international, or STCW, endorsements coincide with the current STCW Certificate.
Exemption	• A Document of Continuity will take the place of renewing a credential. This single document will incorporate all of the capacities that are being placed in continuity status and will have no expiration date.
Security Identification Display Area (SIDA) (*35*)	
Authority	• Executive
Policy	• 49 CFR 1542, 1544. • The SIDA credential provides visual identification of persons in the secure areas.
Program	• The SIDA badge is issued by the local airport after it forwards the required information to the American Association of Airport Executives (AAAE), which then forwards the information to the FBI and TSA. • The SIDA badge is used to monitor individuals who need to have unescorted access to secure areas of airports and aircrafts. In some cases the SIDA badge may identify

Table 3-9. (Continued).

	specific areas that the SIDA badge-holder may enter. For example, at Washington Dulles International Airport (IAD), the badge is color-coded to signify the level of access. • To obtain a SIDA badge, the individual must have a TSA threat assessment, proof of citizenship or immigration status, criminal history check, fingerprints, and personal identification information.
Free and Secure Trade (FAST) (*36*)	
Authority	• Congressional
Policy	• Public Law 109-59 (i.e., SAFETEA-LU); Canada's Partners in Protection Program; and the U.S. Customs-Trade Partnership Against Terrorism Program. • FAST, as part of the Trusted Traveler Program, seeks to enhance border and trade chain security while making cross-border commercial shipments simpler and subject to fewer delays.
Program	• FAST is overseen by U.S. Customs and Border Protection. • FAST expedites the border clearance process for low-risk, pre-approved travelers between Canada and the United States, and between Mexico and the United States. FAST decal holders have access to specially marked lanes at border crossings, thus enabling the holder to avoid back-ups at regular crossing lanes.
NEXUS (*37*)	
Authority	• Congressional
Policy	• Public Law 109-59 (i.e., SAFETEA-LU); Canada's Partners in Protection Program; and the U.S. Customs-Trade Partnership Against Terrorism Program. • NEXUS, as part of the Trusted Traveler Program, seeks to enhance border and trade chain security while making cross-border commercial shipments simpler and subject to fewer delays.
Program	• NEXUS is overseen by U.S. Customs and Border Protection and expedites the border clearance process for low-risk, pre-approved travelers into Canada and the United States for all modes of transportation. • The NEXUS card uses iris recognition biometric technology for persons who arrive in the United States by air. Commercial drivers use a specially marked lane and show their NEXUS membership card in front of a proximity card reader; a visual inspection follows. If arriving by sea, all persons onboard a boat must be NEXUS members in order to take advantage of NEXUS reporting procedures. • Customs is provided with an estimated time of arrival, landing information, origin and destination information, registration information, crew information, and a declaration of all goods being imported, including related currency information.
Secure Electronic Network for Travelers Rapid Inspection (SENTRI) (*38*)	
Authority	• Congressional
Policy	• Public Law 109-59 (i.e., SAFETEA-LU). • SENTRI, as part of the Trusted Traveler Program, seeks to enhance border and trade chain security while making cross-border commercial shipments simpler and subject to fewer delays.
Program	• SENTRI is overseen by U.S. Customs and Border Protection and expedites crossing over the Southwest Land Border (Mexico/United States). The SENTRI card provides expedited processing for pre-approved, low-risk travelers. • Applicants must voluntarily undergo a thorough biographical background check against criminal, law enforcement, customs, immigration, and terrorist databases; a fingerprint-based criminal history check law enforcement check; and a personal interview with a CBP officer. Once approved, applicants are issued identification cards and vehicle decals.

(continued on next page)

Table 3-9. (Continued).

United States Postal Service (USPS) (*39*)	
Authority	• Congressional • Executive
Policy	• USC 3301-3302; 5 CFR 5, 731, 732, 736; and Executive Orders 10450 and 105775. • USPS screening is used to determine USPS employees' eligibility to transport mail and to gain access to mail and mail processing facilities.
Program	• USPS oversees this program and ensures that mail delivery personnel and contractors must also ensure that all persons who require access to mail facilities or drivers are screened. • Individuals are screened every 4 years and are provided with either a non-sensitive or sensitive clearance. Applicants for the non-sensitive clearances must submit to background investigations, fingerprinting, review of a current driving record, and must provide passport-sized pictures. • Sensitive (i.e., public trust) clearances require individuals to complete a separate questionnaire in addition to meeting the requirements of the non-sensitive process. The background investigations are conducted based on questionnaire responses that indicate whether an applicant is reliable, trustworthy, of good conduct and character, and loyal to the United States. Specifically, applicants' current employers are contacted to inquire as to the applicants' adherence to security requirements; honesty and integrity; vulnerability to exploitation or coercion; falsification, misrepresentation, and any other behavior, activities, or associations that tend to show the person is not reliable, trustworthy, or loyal.
Passport (*40*)	
Authority	• Congressional • Executive
Policy	• 8 USC 1185[b] and 22 CFR 53. • On June 1, 2009, the final phase of the Western Hemisphere Travel Initiative (WHTI) *(41)* went into effect for land and sea travel into the United States (requirements for air travel went into effect in 2007). The WHTI is a result of the Intelligence Reform and Terrorism Prevention Act of 2004. • The goal of the WHTI is to facilitate entry for U.S. citizens and legitimate foreign visitors while strengthening U.S. border security.
Program	• Department of State issues passports for the purpose of documenting the identity and nationality of passport holders. The elements of identity are name, date of birth, sex, and place of birth. Most often, nationality and citizenship are congruent. • It is unlawful for any citizen to depart from or enter, or attempt to depart from or enter, the United States without a valid passport. Passports are used to ensure that DHS is able to quickly and reliably identify travelers.
U.S. Department of Defense Common Access Card (CAC) (*42*)	
Authority	• Executive
Policy	• Homeland Security Presidential Directive 12 (HSPD-12). • As of 2008, the Department of Defense had issued more than 17 million cards.
Program	• The Department of Defense began issuing its CAC in October 2006 as a standard ID card that has extensive data storage on an embedded integrated circuit chip that permits rapid authentication and enhanced security for all physical and logical access. • All personnel enrolled in the Defense Enrollment Eligibility Reporting System (DEERS) database are eligible for the card. • Applicants undergo an FBI fingerprint check and a National Agency Check with Inquiries (NACI) background security check.

communicate the identification and authentication information of the credential-holder. Therefore, the results of the security SWOT will be classified as either vetting (assessing the threat/risk of the person) or communicating (conveying identification and authentication). For the purpose of assessing the feasibility of consolidating credentials, the following assumptions were made by the research team to frame the SWOT analysis:

- Assumptions with similarities to current processes
  - The existing issuing agencies would continue to issue the consolidated credential and
  - The processes utilized by the issuing agencies to collect and assess applicant data would remain relatively similar.
- Assumptions with differences to current processes
  - The application process would require a standardized application collecting the same data from each applicant regardless of mode,
  - Each applicant would be vetted to the same level, requiring a full threat assessment (background check, criminal history check, etc.) for each applicant,
  - Each issuing agency would issue the same standardized security credential applicable to all modes and would provide a credential-holder with the ability to access multiple facilities without additional security credentials, and
  - Tiered access to secure areas would be granted using administrative and technical controls established by those individual facilities.

Consolidated Credential—Security SWOT

Credentials with a security focus place emphasis on identifying the credential-holder and ensuring appropriate entry to access-controlled areas. As mentioned, the results of the security SWOT will be classified as either vetting (assessing the threat/risk of the person) or communicating (conveying identification and authentication), as seen in Table 3-10.

The strengths and weaknesses of the SWOT analysis refer to the internal benefits and disadvantages of a process. For the consolidation of the security credentials, strengths and weaknesses refer to the assessment (or vetting) of an applicant's security threat/risk. Conversely, the opportunities and threats refer to the credential's communication of the identity of the credential-holder.

Strengths. A consolidated security credential with a unique serial number used across all modes and by all personnel related to the transportation of hazardous materials would provide an efficient method for tracking credential-holders. This would be beneficial to issuing authorities for the purposes of notification of credential modifications due to policy changes. Furthermore, security is enhanced because credential data could be tracked across facilities and quickly accessed across multiple databases.

Currently, facility credentials have multiple disqualifying offenses, or threats, that they must mitigate. Consolidation of the security credentials would merge many of the threats, creating a minimum threshold to which all applicants would be held accountable. This would create a minimum standard regarding the character of individuals holding this credential.

The consolidation process would require the current assorted procedures for the applicants' risk assessments to be combined, eliminating the need for multiple searches among relevant databases to determine the threat of a single applicant. This would eliminate numerous redundancies for the various agencies while ensuring that the highest level of security is maintained through a minimum-security threshold equal to the most secure individual credential currently in use.

Table 3-10. SWOT analysis results from a security perspective.

Vetting (Internal)	**Strengths** • Better tracking of applicants • Simplifies "threats to mitigate" list • Ensures a minimum threshold for security • Quickly adapts policy for new threats	**Weaknesses** • Institutional resistance • State and federal legislative actions required • International issues • Decreased resolution regarding the "threats to mitigate" list
Communicating (External)	**Opportunities** • One credential for end-user • Uniform look and design on the credential • Simplifies training for security personnel • Only one issuing agency to notify if problems arise	**Threats** • Increased ability to abuse/misuse

There also would be an added benefit related to policy adaptation. When necessary, a single credential falling under a single policy could be adjusted quickly to adapt to new threats. This would create a much more efficient system, enabling all modes and all facilities to quickly react to the most current security threats. Additionally, by having a single credentialing system, a credential-holder would need to report the loss of a credential only once to facilitate the notification across all modes and all facilities of a potential security breach. This single point of contact would drastically improve the speed with which the entire system counters a potential threat.

Weaknesses. The primary weakness of a consolidated approach would be the implementation issues typically associated with the establishment of a new process. A single credential would be applicable to many facilities under the control of multiple agencies. Therefore, the consolidated security credential would require effective communication and cooperation across multiple agencies to address administrative and policy issues and ensure successful implementation.

For those security credentials designed for border crossings (i.e., passport, FAST, NEXUS, SENTRI), there are disadvantages with attempting to consolidate with domestic security credentials. Those credentials that are intended to be used at border crossings have a different focus than the remaining security credentials. This subdivision among the security credentials creates complexity from a consolidation perspective. For example, the disqualifying offenses for the passport are focused on very different threats as compared to the disqualifying offenses for the facility security credentials.

The consolidation of the disqualifying offenses, or threats to mitigate list, may result in a loss of function-specific focus. Each current credential is designed with a given intent and specific threats.

Opportunities. The most obvious opportunity is the generation of a single security credential that would allow the end-user to access controlled areas of multiple facilities (e.g., marine ports, airports, and rail yards) without the need to apply for, and acquire, a new credential at each facility. The credential-holder would only need to maintain one security card, which will result in numerous economic advantages that will be discussed in the cost-effectiveness SWOT analysis.

A single credential would possess a uniform design and look. From a human factors perspective, a standardized look facilitates universal recognition across participating facilities. This increases awareness and propensity for security challenges to the credential-holder. A positive result of this uniform look is the simplification of training for security personnel. In all modes, and at all facilities, the security personnel will evaluate the same credential.

A consolidated credential would streamline the process for notifying an issuing agency of problems (e.g., loss, theft) of the security credential. With the current credentialing process, the credential-holder must contact numerous issuing agencies if problems arise. With only one security credential, the credential-holder would need to only contact one agency to resolve any problems that occur.

Threats. As previously stated, a single facility security credential would provide access for applicable personnel to multiple facilities, thereby easing the process for those personnel; however, this is also a threat in that it would create a "single key" scenario. That is, someone who possesses a valid consolidated security credential could potentially access other facilities for illegitimate purposes. Also, should the credential be compromised (i.e., counterfeited) it could be used to access more facilities than any currently existing credential. Credential abuse or misuse is certainly a threat; however, there is the potential to combat this issue using administrative controls on a need-to-access basis.

Based on the results of the SWOT analysis from a security perspective, the research team concluded that the intent of several security credentials (i.e., U.S. passport, FAST, NEXUS, and SENTRI) is too varied to be considered equal to the remaining security credentials. These four security credentials are focused on the identification of the credential-holder at border crossings; the remaining credentials are focused on identification and facility access. Therefore, the original model was revised to reflect this additional (third) category, as shown in Figure 3-20.

Consolidated Credential—Cost-Effectiveness SWOT

The final SWOT analysis for a consolidated credential focused on cost-effectiveness for a consolidated security credential and a consolidated safety credential. The evaluation focused primarily on the increased or decreased costs associated with a consolidated credential for both the issuing agencies (strengths/weaknesses) and potential credential-holders (opportunities/threats). The results are included in Table 3-11.

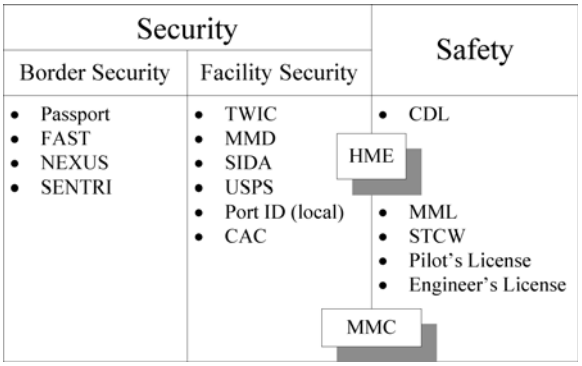

Figure 3-20. Revised model of categorized credentials.

Table 3-11. SWOT analysis results from a cost-effectiveness perspective.

Vetting (Internal)	**Strengths** • Eliminates redundancies for issuing agency • Decreases training requirements for security personnel	**Weaknesses** • Requires new or additional technology
Communication (External)	**Opportunities** • Eliminates redundancies for credential user • Increases availability of enrollment centers(*43*)	**Threats** • None identified

Strengths. The primary strength of a consolidated credential is the elimination of cost redundancies. Currently, each credential application must be handled and processed as if it represents a unique individual. For example, an individual applying for two credentials would be required to complete two separate applications, including two security threat assessments. Reducing the number of applications will directly result in a decrease in time and effort required by the issuing agencies.

A single credential with a uniform look and design could facilitate a faster and more simplified training program for security and inspection personnel.

Weaknesses. Because additional technology will be required (as was needed for the TWIC) across all modes to fully utilize the consolidated credential, there will be an increase in cost to the individual facilities. This cost is potentially significant if the technology required is not currently in use and must be acquired by all facilities for all transportation modes. An example would be a card reader that must be installed at each gate of all ports, airports, and other secure facilities, in police cars, weigh stations, and any other inspection facility.

Opportunities. The most apparent and potentially significant opportunity for consolidation is the elimination of redundancies from the perspective of a credential-holder. The elimination of multiple applications and the associated fees, the reduction in time requirements associated with filling out and submitting multiple applications, and the elimination of numerous trips to facilities (for application, fingerprinting, and receiving the credential) will result in significant cost savings for credential-holders. In addition, most existing credentialing centers could be available to all applicants regardless of transportation mode, decreasing travel times, and increasing availability of resources.

Threats. The consolidated credential approach presented no specific cost-related issues for the credential user.

Non-Consolidated Credential Approach

The research team used a SWOT analysis to evaluate the non-consolidated credential option (the current system) to allow for comparisons. In the same manner, the SWOT analysis for the non-consolidated credential approach was conducted from both a security and cost-effectiveness perspective.

Non-Consolidated Credential—Security SWOT

The results of the security SWOT will be classified as either vetting (assessing the threat/risk of the person) or communicating (conveying identification and authentication) as seen in Table 3-12.

Strengths. As seen in the requirements-to-obtain and disqualifying offenses sections, each issuing agency assesses the threats specific to its concerns for each of its applicants and can afford to do this due to the limited information required. By focusing its assessment and limiting the information to what is necessary for its purposes, the issuing agency can assess each applicant with greater resolution, which results in enhanced security.

Weaknesses. With multiple credentials and corresponding issuing agencies, the threat increases that a credential-holder is deemed an unacceptable risk by one agency and the information will either be delayed or never reach other agencies (or facilities) due to the complexities of sharing such information across multiple data platforms and agency facilities.

Opportunities. The amount of information placed on each credential varies based on the issuing agency, the type, and purpose of each. Where a consolidated credential would need to contain the information necessary for all purposes, non-consolidated credentials can be specifically tailored for their purposes. This design allows for immediate recognition for

Table 3-12. SWOT analysis results from a security perspective (non-consolidated approach).

Vetting (Internal)	**Strengths** • Focused applicant assessment	**Weaknesses** • Complexity of information sharing • Inconsistent vetting processes(*30*) • Re-vetting of the same people(*30*) • Inefficient information and data collection(*30*) • Data collection or processing errors(*43*)
Communication (External)	**Opportunities** • Tailored credentialing	**Threats** • Variance in credential appearance

security personnel, as well as for fellow employees within a challenge program.

Threats. Inherent in a credentialing system with multiple credentials issued by multiple agencies is variance in the appearance of the credentials. When referring to multiple modes of transport and multiple facilities, the variance of these security credentials can increase the risk of fraudulent credentials being successfully used to gain access to a secure facility. Although technology exists to combat this threat, a non-consolidated system allows each issuing agency to decide what type of credential should be developed.

Non-Consolidated Credential—Cost-Effectiveness SWOT

The non-consolidated credential approach evaluates the cost-effectiveness from both an issuing agency perspective (strengths and weaknesses) and the perspective of the credential-holder (opportunities and threats). The SWOT results are provided in Table 3-13.

Strengths. From a cost-effectiveness standpoint, no specific strength for the issuing agency was identified.

Weaknesses. For each applicant there is an associated cost to process the application and any related threat assessments. For the non-consolidated credential approach, the same applicant will need to apply multiple times to gain access to certain facilities. Although some portion of each application may be unique, the security threat assessment portion will not be distinctive. Each additional search for an applicant raises the cost of administration, adds to the list of applicants to assess, and potentially delays the process.

Opportunities. No specific opportunities for improved cost-effectiveness for credential users were identified.

Threats. Similar to the additional administrative costs for each agency related to the need for multiple credentials, the costs to the potential credential-holder are also increased. These additional costs will result from multiple applications, fingerprinting, trips to an issuing agency, and time required to fill out applications.

Because of the multiple designs and features of the individual credentials, to ensure security, facilities will need to provide specialized training (at additional time and cost) for the recognition and monitoring of these unique details.

Table 3-13. SWOT analysis results from a cost-effectiveness perspective (non-consolidated approach).

Vetting (Internal)	**Strengths** • None identified	**Weaknesses** • Increased administrative costs • Multiple enrollment centers and forms
Communication (External)	**Opportunities** • None identified	**Threats** • Multiple credential costs • Multiple enrollment centers and various forms • More training for facility security personnel

Consolidation Options Analysis

Each of the existing security credentials within the current transportation system has a unique purpose and has been developed with that specific purpose in mind. The combination of credentials requires that the consolidation still functions for its intended purpose. Therefore, the research team broke down each current credential (and acquisition/application process) into the very elements constituting the credentials (see Table 3-2, Table 3-4, Table C-1, Table C-2, and Table C-3). This allowed for an evaluation of basic credential "building blocks." The research team then combined candidate credentials in various options (shown in Table 3-14), which resulted in new combinations of elements.

The options were developed through dialogue with the TAG, results of the online survey instrument, and as a result of the Phase I analysis. Option 1 consisted solely of the TWIC due to suggestions that the TWIC should be considered as a standalone solution for consolidating security credentials for transportation workers. The results of the Phase 1 analysis showed the TWIC to be potentially limited as to its applicability in all modes. Potential limitations were due to the assumption that each credential's identified elements are necessary for it to function as a security credential. When a comparison was made, it was determined that the TWIC had very few elements in common with other credentials. The results of this comparison were presented accordingly in the elemental matrices. Option 2 (TWIC, MMD, SIDA, USPS, CAC) was simply the combination of all credentials that appeared to show promise for successful consolidation based on the Phase I analysis. This combination of all credentials deemed feasible for consolidation provided the upper bounding of required elements and functionality. Therefore, Option 2 captured each unique element and the associated background checks necessary for a consolidated credential replacing five credentials, and covering all four transportation modes. Option 3 (TWIC, MMD) was chosen to evaluate the consolidation of two credentials currently being used within the marine mode. An evaluation of this combination of credentials could determine if there is more potential for success within a given mode, or regardless of mode. Option 4 (TWIC, SIDA, CAC, MMD) comprised all of the elements of Option 2 except the USPS credential. The results of the research indicated that the USPS was held quite infrequently, and does not have a significant role in HazMat transportation. Therefore, Option 4 was designed to evaluate the impact of this credential on the overall consolidation process. It is important to note that the CDL-HME as a whole is a vastly different type of credential; however, for purposes of inquiry and comparison, the security portion of the HME could be viewed as equivalent to the TWIC because of the many similarities between the two credentials.

Table 3-14. Credential combinations evaluated as consolidation options.

Credential Options Evaluated	
TWIC	Option 1
TWIC, MMD, SIDA, USPS, CAC	Option 2
TWIC, MMD	Option 3
TWIC, SIDA, CAC, MMD	Option 4

Following the development of the consolidation options, a list of required attributes and requirements to obtain were developed for each credential containing the unique sets of elements established by the credentials comprising each option. This set of elements specific to each option was then used to evaluate applicability for use by HazMat transportation workers in all modes. Table 3-15 contains the unique elements required of the applicant to obtain the credentials within a given option. This comparison provides the unique list of requirements necessary of a consolidated credential to replace the credentials comprising each option.

In all, there are 40 elements that make up the unique requirements to obtain for a consolidated credential to replace Option 2. This assumes all elements currently existing and pertaining to the individual credentials would be necessary in a consolidated system. This list of elements provides a template for a consolidated credential with regard to the pieces of information to be collected from the applicant. In Table 3-16, the unique list of attributes is shown with the corresponding notations of applicability for each option.

There are 24 unique attributes applicable to consolidation; of course, each is accounted for in Option 2, which is comprised of all candidate credentials. There is certainly variation in the applicable attributes per option; however, Options 2 and 4 are exactly the same. The sole difference between these two options is the lack of the USPS credential in Option 4, which did not include a single unique attribute beyond those already accounted for in the other candidate credentials within Options 2 and 4. Again, this complete list of unique attributes provides the minimum standard for a consolidated credential replacing each existing credential within Option 2. Finally, Table 3-17 includes the unique background checks for each option and corresponding notations of applicability.

All but Option 1 contain all four background check processes noted. This similarity among security credentials provides a logical starting point for consolidation. As evidenced by the data, little-to-no change is required to the background check process should consolidation of the candidate credentials occur. It is important to note that although the processes are the same (in most cases), the disqualifying offenses are not. Therefore, this logical beginning is not without required compromise. Should consolidation occur, the disqualifying offenses would need to be standardized. This process could raise all applicants to the highest standard, theoretically increasing security systemwide. However, this would most certainly restrict

Table 3-15. Unique requirements to obtain for consolidation.

Option	1	2	3	4
Address	●	●	●	●
Address History		●		
Aliases	●	●	●	●
Character References		●	●	●
Citizenship Information	●	●	●	●
Copy of Driver's License		●		
Date of Birth	●	●	●	●
Drug Testing		●	●	●
Education History		●		
E-Mail Address	●	●	●	●
Employer Fax Number	●	●	●	●
Employer's Address	●	●	●	●
Employer's Name	●	●	●	●
Employer's Phone Number	●	●	●	●
Employment History		●		
Eye Color	●	●	●	●
Fax Number	●	●	●	●
Fingerprinting	●	●	●	●
Full Name	●	●	●	●
Hair Color	●	●	●	●
Hearing Test		●	●	●
Height	●	●	●	●
Medical/Physical Examination		●	●	●
Military Service		●		
National Driver Register Check		●	●	●
Next of Kin		●	●	●
Next of Kin E-Mail Address		●	●	●
Next of Kin Phone Number		●	●	●
Occupation	●	●	●	●
Phone Number	●	●	●	●
Place of Birth	●	●	●	●
Preferred Notification Method	●	●	●	●
Race		●		●
Previous Screening within 12 months		●		
Security Threat Assessment	●	●	●	●
Sex	●	●	●	●
Social Security Number	●	●	●	●
Sponsoring Agency Information		●		●
Vision Test		●	●	●
Weight	●	●	●	●

Table 3-16. Unique attributes for consolidation.

Option	1	2	3	4
Access Level		●		●
Address		●	●	●
Authorization Agency		●	●	●
Bar Code		●		●
Citizenship		●	●	●
Date of Birth		●	●	●
Date of Expiration	●	●	●	●
Date of Issue		●		●
Dual Interface ICC	●	●	●	●
Employer		●		●
Endorsements		●	●	●
Eye Color		●	●	●
Full Name	●	●	●	●
Hair Color		●	●	●
Height		●	●	●
If Found		●		●
Issuing Location/Branch		●	●	●
Magnetic Strip		●		●
Photograph	●	●	●	●
Signature		●	●	●
Social Security Number		●	●	●
Tamper-Resistant Features	●	●	●	●
Unique Serial Number		●	●	●
Weight		●	●	●

the applicant pool and dramatically reduce the labor force. Conversely, the standard could be set to the least common denominator, potentially lowering overall security, but increasing the applicant pool sufficiently to handle labor demand. Realistically, this process would result in some sort of middle ground.

It is also possible that the variation in disqualifying offenses could be used to develop a tiered consolidated credential. The tiers would need to be defined by appropriate stakeholders based on risk analysis, labor requirements, and job function. It is impractical to establish tiers that could allow credential-holders to perform part, but not all, of their required job function.

The options were evaluated to determine the strongest possibility for success in consolidation. To that end, Option 2 as a consolidated credential would provide the broadest applicability. (This is expected because it is comprised of the most candidate credentials.) However, the process of consolidation must consider more than just the broadest applicability with regard to credential elements and processes. It must also consider the cost of change. Each option (except Option 1) would require the consolidation of credentials issued by different agencies. The consolidation of personnel, facilities, and back-

Table 3-17. Unique background check elements for consolidation.

Option	1	2	3	4
Fingerprint-Based Criminal Records Check	●	●	●	●
Name-Based Relevant Database Check	●	●	●	●
Drug Test		●	●	●
National Driver Register Check		●	●	●

ground processes, as well as the credentials themselves, would require certain costs. It is possible that in some cases the act of consolidation could result in cost savings associated with some aspect of the overall credential process. This information should be understood before a definitive decision could be made on the best course of action regarding consolidation. As is often the case, the costs associated with the various options for consolidation could significantly change the perspective of stakeholders, ultimately changing the ideal option from one to another.

In addition to understanding the costs associated with potential consolidation it is important to understand the effect that consolidation could have on existing stakeholders, and the likelihood for successful adoption and use. In order to inform this discussion, it was necessary to evaluate policy impetus as it relates to the process of consolidating security credentials for persons who transport hazardous materials.

Policy Implementation Analysis

The following discussion draws upon organizational change, organizational learning, and policy implementation research, and presents a multiple-perspective analysis (i.e., organizational, technical, and personal). Multiple-perspective analysis is designed to deal with ill-structured policy problems employing a systematic evaluation of policy solutions.(*6*)

Organizational Perspective

The characteristics of the organizations in question must be taken into account when policy changes are proposed. Organizational characteristics to be considered are impetus and authority, organizational form, and competitive isomorphism.

Impetus and Authority. The impetus for policies and/or an organization can come from a variety of sources including federal legislation, rulemaking, executive authority, or local authority. Congress, through legislative action, can create the impetus for particular policies and/or the organization itself. Regulatory impetus refers to those policies that have been established by agencies through the rulemaking process. Executive authority indicates the impetus originated with an executive order. Local authority refers to those policies established by state, local, or regional special authority (for example, the establishment of a port authority and subsequent port operating procedures). Table 3-18 provides an overview of the relevant credential, and its authority.

Organizational Form. Jensen (*44,* p. 110) defines organizational form as a particular organization type that has a specific policy purpose and mission. For example, the DHS implements policies related to homeland security. Jensen also notes that organizations tend to have an institutional basis or a technical basis, while often combining elements of both. Organizations with an institutional basis "are derived more from values and meanings of society and less on technical activities, efficiency, or rationality."(*44,* p. 114) An example of an institution basis is a port when it operates to implement shipping policies. Institutional-based policy decisions may be contentious. As a result, policy changes may require resolution from the political system. Changes may need to be dictated by the legislator, which acts as the moderator of large-scale change (*44*). Without legislative intervention, proposed policy changes may face significant resistance.

Organizations that have a technical basis tend to focus on efficiency or have a production basis. As Jensen notes, these agencies exist to fulfill a concrete need and to improve efficiency.(*44*) For example, departments of motor vehicles exist

Table 3-18. Credentialing agency's impetus and authority.

Credential	Impetus	Authority
FAST	Congressional	Public Law 109-59 (i.e., SAFETEA-LU)
Local Ports	Local Authority	Based upon state, local, or regional special authority (i.e., port authority)
MMC	Executive	46 CFR Part 10
MMD	Executive	33 CFR 101-146 and 46 CFR Parts 10-16
NEXUS	Congressional	Public Law 109-59 (i.e., SAFETEA-LU)
Passport	Executive and Congressional	8 USC 1185[b] and 22 CFR 53
SENTRI	Congressional	Public Law 109-59 (i.e., SAFETEA-LU)
SIDA	Executive	49 CFR 1542, 1544
TWIC	Congressional	Maritime Transportation Security Act of 2002, Public Law 107-295 and 46, USC 70195
U.S. Department of Defense CAC	Executive	Homeland Security Presidential Directive 12 (HSPD-12)
U.S. Postal Service	Executive and Congressional	USC 3301-3302; 5 CFR 5, 731, 732, 736; and Executive Orders 10450 and 105775

to implement and enforce motor vehicle policies. Technical needs may be internal to organizational units and may differ significantly among organizations. Continuing the state departments of motor vehicle example, policies and procedures within each state may vary and may use differing technologies. Table 3-19 provides an overview of credentials and associated organizational forms.

Technical Perspective

The technical perspective considers the climate in which the organization exists, financing, risk, and technological trends.

Organizational Climate. Organizational climate requires that one account for the intangible feelings of political power, institutional legitimacy, and social fitness. The competition for power and legitimacy may be manifest in difficulties in reconciling differing requirements of specific policies into a new set of standards and determining responsibility for the new policy. A number of agencies, in response to agential concerns, developed the current credentials. As a result, the underlying justifications for these credentials vary. For the FAST, Local Ports, MMD, NEXUS, U.S. passport, SENTRI, SIDA, TWIC, and CAC, the underlying justification is security. For the MMC, the underlying justification is to ensure skill, knowledge, and security. For the USPS credential, the underlying justification is to ensure fitness for duty and security.

Likewise, agency stakeholders hold certain expectations in regard to each credential's function and administration. Changes to current policy may be viewed as a challenge of an organization's power within the policy subsystem or as a challenge to the organization's legitimacy. To manage uncertainty, cross-functional teams should be included in the development of the new policy from the earliest stage possible. These cross-functional teams should represent members of all departments (e.g., management, data processing, information technology)

Table 3-19. Credential and associated organizational form.

Credential	Organizational Oversight	Institutional or Technical Predominant Basis
FAST	Canada Border Service Agency and U.S. Customs and Border Protection Agency	Technical—charged with enforcing customs and border policies
Local Ports	Local Authority	Institutional—develops and implements policies beneficial to the operation of the local concern
MMC	U.S. Coast Guard	Institutional—charged not only with providing for the national defense, but also with developing operational guidelines that are consistent with institutional norms
MMD	U.S. Coast Guard	Institutional—charged not only with providing for the national defense, but also with developing operational guidelines that are consistent with institutional norms
NEXUS	U.S. Customs and Border Protection Agency	Technical—charged with enforcing customs and border policies
Passport	Bureau of Consular Affairs (CA)	Technical—as a unit of the Department of State, CA is charged with protecting the lives and interests of American citizens abroad and strengthening the security of U.S. borders through the vigilant adjudication of visas and passports
SENTRI	U.S. Customs and Border Protection Agency	Technical—charged with enforcing customs and border policies
SIDA	Transportation Security Administration	Technical—as a unit of DHS, charged with protecting the nation's transportation systems to ensure freedom of movement for people and commerce
TWIC	Transportation Security Administration	Technical—as a unit of DHS, charged with protecting the nation's transportation systems to ensure freedom of movement for people and commerce
U.S. Department of Defense Common Access Card	U.S. Department of Defense	Institutional—charged not only with providing for the national defense, but also with developing operational guidelines that are consistent with institutional norms
U.S. Postal Service	Independent executive agency established within the U.S. Constitution	Technical—charged with the task of mail delivery

Table 3-20. Credential stakeholders.

Credential	Credentialing Agency and Affiliated Agencies	Credential User Stakeholders
FAST	Canada Border Service Agency and U.S. Customs and Border Protection Agency and U.S. Department of Homeland Security	Supply-chain members including commodity shippers, truck drivers
Local Ports	Local Authority	Individuals seeking access to ports including longshoremen, truck drivers, port employees, vessel crews, outer continental shelf facility workers, merchant mariners
MMC	U.S. Coast Guard	Crewmembers of U.S. ships with a GRT of more than 100 tons
MMD	U.S. Coast Guard	Crewmembers of U.S. ships with a GRT of more than 100 tons
NEXUS	Canada Border Service Agency and U.S. Customs and Border Protection Agency and U.S. Department of Homeland Security	Supply-chain members including commodity shippers, truck drivers, crews of shipping vessels and airplanes, facility managers
Passport	Bureau of Consular Affairs (CA) and U.S. Department of State	Individuals attempting to depart from or enter the United States
SENTRI	Canada Border Service Agency and U.S. Customs and Border Protection Agency and U.S. Department of Homeland Security	Supply-chain members including commodity shippers, truck drivers
SIDA	Transportation Security Administration and U.S. Department of Homeland Security	Individuals who need unescorted access to secure areas of airports and aircrafts, airport management, airlines and other shippers
TWIC	Transportation Security Administration and U.S. Department of Homeland Security	Individuals seeking access to ports including longshoremen, truck drivers, port employees, vessel crews, outer continental shelf facility workers, merchant mariners
U.S. Department of Defense CAC	U.S. Department of Defense and U.S. Department of Homeland Security	Members of the armed services, civilian employees, government contractors
U.S. Postal Service	USPS	Postal employees and vendors

and organizations affected by the new policy. Consolidated credentialing efforts will require a number of agencies and departmental units to work together to address the needs of a variety of stakeholders. A brief summary is presented in Table 3-20. This list of stakeholders is meant to provide a macro-level view of the stakeholders that should be involved in credential consolidation discussions and efforts.

Financing. Waldron notes that cost of change is a major barrier to the implementation of new policies.(*45*) Cost and financing concerns include the more tangible costs associated with competition over scarce resources and customers. Examples of financial considerations include current and future policy revenue streams (or lack thereof); cost of equipment and technologies; cost of time to develop, test, and implement new policies; and training costs associated with new policies. Looking at only the cost of each credential, it can be seen that the consolidation of credentials may have a significant impact on the agency's revenue generation stream (see Table 3-21).

Risk. Risk refers to the balancing of policy details with financial constraints. Trust is also a consideration. Trust issues can manifest in the lack of trust between participating organizations or a lack of trust in the policy results. To address trust issues, the development and implementation of a consolidated credential will require that stakeholders work together to ensure that program needs are addressed, guidelines are established, and outcomes are met.

Technology Trends. Technology trends require that one accounts for the testing of new systems, the continued usefulness of current systems, and potential problems relating to the timing of the change to a new system and general coordination of that change. It is critical that policy change activities be coordinated in the overall policy network. There must be a clearly communicated understanding of the new operation system if implementations are to be limited. Additionally, organizational units must demonstrate cooperation and a willingness to work together in order to facilitate a systemwide policy change. When making software and hardware decisions, users

Table 3-21. Credential stakeholders and associated costs.

Credential	Credentialing Agency and Affiliated Agencies	Stated Credential Cost
FAST	Canada Border Service Agency and U.S. Customs and Border Protection Agency	$50.00
MMC	U.S. Coast Guard	$100.00
MMD	U.S. Coast Guard	$100.00
NEXUS	U.S. Customs and Border Protection Agency	$50.00
Passport	Bureau of Consular Affairs (CA) and U.S. Department of State	$100.00
SENTRI	U.S. Customs and Border Protection Agency	$122.25
SIDA	American Association of Airport Executives	$91.33*
TWIC	Transportation Security Administration	$132.50
U.S. Department of Defense CAC	U.S. Department of Defense	Unavailable
U.S. Postal Service	USPS	Unavailable

*Note: Arithmetic mean, see Appendix F.

should compare packages, obtain feedback from current users, and work closely with the support personnel and line workers who will be the end-users of the technologies.

The implementation of a consolidated credential will require the adoption of new hardware and software. As noted in the attribute overview, credentials may include bar codes, RFID, dual interface integrated circuit chips (ICC), and magnetic strips. The information contained in these technologies provides not only a redundancy of visible information on the credential, but also may incorporate biometrics not included anywhere else on the credential (e.g., the TWIC credential-holder's fingerprint, which is available by accessing the ICC). Agencies have dedicated funding to establish the current technologies to make and process the credentials and to maintain the data associated with the credentials. Each facility also incurs costs to accommodate the credentials. These costs not only include infrastructure costs, but also the costs associated with training employees on the new technologies.

Personal Perspective

Just as organizations may be resistant to change, individuals within those organizations may also be resistant to change. Resistance to change can be seen at all layers of the hierarchy—from management to front-line employees. When dealing with the consolidation of programs, the need to address the sources of resistance is paramount. Waldron identifies several sources of resistance including the fear of change, difficulty in changing, fear of new technology, lack of belief in the changes, lack of patience for the benefits of change, concern for job security, and opposition to new tasks.(*45*) Waldron also identifies several methods for overcoming change. These methods include obtaining assistance from outside parties, formalizing procedures, initiating quality assurance policies, embracing a model conducive to continual modifications and supplemental changes, and training regarding the benefits of the change as well as for new tasks.(*45*)

CHAPTER 4

Conclusions and Suggested Research

Consolidating Credentials

Hazardous materials are transported *from* many locations *to* many locations throughout the United States on a daily basis. These materials originate at chemical manufacturing facilities, tank farms, and other refining and manufacturing locations. They also originate outside the United States and are imported through border crossings and port facilities. Hazardous materials are used every day in the manufacture of products consumed within the United States. To facilitate the manufacture of so many products using these hazardous materials (often purified raw chemicals), materials are transported by rail, highway, through marine ports, as cargo through airports, and—in some cases—by pipeline. It is this system of infrastructure in all modes, the facilities, and the vehicles of transport that constitute the HazMat transportation system.

Hazardous materials by definition pose a potential risk to health, safety, and property when transported.(*46*) Thus, it is prudent to maintain a certain level of security throughout the HazMat transportation system to limit or prevent negative outcomes from this necessary part of the overall economic structure. The HazMat transportation system can be simplified by observing its three basic parts—origin, transport, and destination. That is, the process may have multiple points of origin and multiple legs of transport; however, there is always a start and finish requiring a path in between. By achieving security in all three portions of the system, the entire system can be considered secure. Although this description is very basic, the overall concept remains constant. This research focused largely on the security credentials used to gain access to the points of origin and/or destination (and intermediary facilities along the transport pathway).

The majority of the identified security credentials serve as a means for securing these facilities with the ultimate goal of preventing negative consequences associated with misuse of hazardous materials. Additionally, security of the facilities helps to prevent disruption to their operations, ensuring continuous, economically positive existence. This level of security is accomplished largely by understanding who, and what, is accessing the facility. Security credentials provide this necessary information in the following two ways:

- Vetting the individual credential-holder and
- Communicating pertinent information for facility access control.

The security credentialing process requires two parties—the applicants (who become credential-holders if approved) and the issuing agencies. The issuing agencies are burdened with collecting and storing personal information, adjudicating cases, and bearing the costs associated with these efforts. The applicants are burdened with providing personal information in the proper format and the associated costs.

For the purposes of this research, a credential was defined as portable documentation to validate one's identity and/or skill set. With that in mind, 19 credentials were identified as required of persons who transport hazardous materials. Fifteen of these are designated security credentials with the purpose of (1) ensuring someone does not pose a security threat, (2) validating lawful status in the United States, and (3) verifying identity. Many of these security credentials share common requirements to obtain (i.e., name, date of birth, citizenship information, address, security threat assessment, gender, Social Security number, phone number, aliases, height, eye color, hair color, and employer name) and attributes (i.e., full name, date of expiration, photograph, tamper-resistant features, unique serial number, date of birth, citizenship, and sex).

Currently, a single transportation worker (e.g., truck driver, port employee, or rail engineer) may be required to carry in excess of five security credentials in the course of his/her employment and associated duties. Each of these credentials requires a specific cost, and an investment of time to acquire. Additionally, the issuing agencies must manage the data collection and data storage associated with that single transportation

worker's multiple credentials. This system is the result of multiple factors associated with the creation of credentials. In some cases, the credentials were developed to prove the capabilities of the credential-holder, and in other cases, the credentials were developed for the purposes of security. Each credential was designed for a specific mode, facility, or a combination of both. Some are required by the entity having authority over the facility; others are federally mandated. On the surface, the system appears to have significant redundancy by requiring the same personnel to maintain multiple credentials. However, each credential (with the exception of the TWIC and MMC) is specific to its purpose and was designed independently of the others. This has led to a system that has nearly as many credentials as it does specific security needs (and in some cases includes the need to prove a certain skill set such as the MML, STCW, or CDL).

In addition to the many unique needs requiring different credentials, there is the information necessary to ensure that security credentials are verifiable. That is, security credentials that are all specifically focused on ensuring identity and low-risk histories are duplicated due to multiple issuing agencies and a lack of data sharing. This is evident when evaluating the nation's marine ports, where individual ports typically manage their own security and, thus, many developed their own security credential.

The primary purpose for this research was to determine if it is feasible to consolidate security credentials and, if so, how this could be accomplished. This evaluation included each of the tasks described in the research approach section of this document, and resulted in the data contained in the results section of this document. The Phase I findings of the elemental analysis, time and costs analysis, regulatory analysis, and SWOT analysis indicated that the consolidation of several security credentials required of persons who transport hazardous materials would be feasible, including the CAC, MMD, SIDA, TWIC, and USPS.

In Phase II, four options for consolidation were considered. This effort provided insight into the minimum elements and background processes required of a consolidated credential in order to remain consistent with existing security credentials. The evaluation provided the 64 unique elements necessary for a consolidated credential to replace all candidate credentials. It also demonstrated the similarities of the background check processes for all of the candidate credentials. It will be necessary to perform a full cost-benefit analysis to fully understand the costs associated with the various consolidation options. It also will be important to understand policy impetus as it relates to the potential consolidation of security credentials. The Phase II effort considered consolidation with regard to both existing data and needed data. However, it is also important to consider the policies and protocols of security credentials. HSPD-12 established requirements for federal departments and agencies to strengthen security and efficiency through the use of a standardized security credential. The threats mitigated by this directive are not significantly different from the threats facing the HazMat transportation sector. Therefore, the very same principles and justifications outlined in the HSPD-12 are applicable to the transportation sector, specifically the portion of the transportation sector that is involved with hazardous materials. HSPD-12 acknowledges the need to eliminate "variations in the quality and security of forms of identification used to gain access to secure federal and other facilities where there is potential for terrorist attacks . . ."(*47,* p. 1) As a result of HSPD-12, the National Institute of Standards and Technology (NIST), by charge of the directive requiring the secretary of commerce to oversee the effort, developed the Federal Information Processing Standards (FIPS 201 and, subsequently, FIPS 201-1).(*48*) This standard satisfies the technical requirements of HSPD-12, improving the identification authentication related to accessing federal facilities and information systems.

Further action was taken by NIST to develop the Personal Identity Verification (PIV) Program. This program includes a set of specifications that standardize the identification data types and protocols for transfer of data related to security credentialing. The PIV Interoperability (PIV-I) specifications allow for entities outside of the federal government to participate at the same level. The PIV (and PIV-I) Program provides a growth-enabled framework within which to develop long-term, multimodal, and applicable, security credentials. This allows for streamlined efficiency, data sharing, and the maintenance of security. Ultimately, the use of standards could allow for multiple security credentials that can function across platforms. This could lead to an elimination of multiple credentials for one person—instead, one credential could provide access to multiple facilities. Serious consideration should be given to the adoption of PIV (or similar) specifications and protocols for HazMat-specific security credentials.

Each of the credentials to be consolidated has been designed for a specific function by the various issuing agencies. This level of specificity is based on the perceived need to tailor each credential for the individual requirements of the issuing agencies. The results of this research indicate that a consolidated security credential can be broadly applicable if appropriately designed. Additionally, as indicated in the regulatory analysis results, consolidation of security credentials across issuing agencies presents logistical issues such as cross-agency data storage and access. Finally, a determination must be made as to whether one agency issues the consolidated credential or if multiple agencies issue a standardized security credential.

The decision regarding whether to implement a consolidated credential and the form that credential should take will be complex. As discussed, the implementation of a consolidated credential will require the input of a wide range of parties including agency officials, credential-holders, business

owners, port operators, security personnel, and others as appropriate. Because of the number of stakeholders involved, it is necessary to view potential solutions from organizational, technical, and personal perspectives. Issues within each perspective are not mutually exclusive and may require analysis from a holistic perspective. Additionally, because of the complexities associated with the development of a new credential and the multi-jurisdictional nature of current credentialing systems, the authority for a new credentialing policy may need to come from a source above the agencies (i.e., executive order or legislation). Congressional and executive sources may be able to facilitate the diverse interest in a manner that will ensure the successful implementation of a consolidated security credential.

Consolidating Background-Check Processes

In addition to the potential consolidation of security credentials for persons who transport hazardous materials, this research also evaluated the possibility of consolidating background check processes. The analyses also demonstrated that several security credentials required for HazMat transport have background assessment redundancies that could be evaluated for possible elimination; these include FAST, NEXUS, SENTRI, CDL-HME, MMC, and passport, in addition to the five credentials considered as candidates for consolidation. There is strong evidence that the background check processes for these credentials could be standardized and applicable across all transportation modes.(*2*) As shown in Table 3-3, 10 of the 11 credentials identified shared both a fingerprint background check (i.e., required for all but the passport) and a name-based background check (i.e., required for all but the USPS). In some cases there are minor variations in how these processes are completed or which databases are checked; however, the overall processes are extremely similar. More importantly, the objective of these background checks (i.e., identifying any disqualifying offenses) is the same for all credentials.

The premise for this research was concern over the redundancies of the security credentialing system for persons who transport hazardous materials. Based on the research, it is apparent that consolidation of existing credentials requires significant change to the current security credentialing system and could meet with organizational or institutional resistance. It is believed that the consolidation of background checks would deal largely with the application process, and would be transparent to the end user. An example of acceptance for other credential vetting processes would be the TWIC and the HME, where a cost reduction is applied to applicants already holding a CDL-HME when they apply for the TWIC. There are restrictions on this agreement; however, it provides a starting point. Ultimately, this system of reciprocity could be extended to the majority of credentials identified here.

A system where background check processes are standardized could reduce cost due to increased efficiency. Multi-agency data sharing could also streamline the process for all stakeholders. This system would require that the results of a credential application be applicable to a secondary credential application regarding the background investigation. As is currently the case, it would likely require the expiration of any subsequent credentials to coincide with the time limit of applicability associated with the first credential. That is, if an applicant is granted a TWIC in 2010, and then applies for a FAST card in 2012 using the background check from the TWIC application, the FAST card would also expire in 2015. Initially, this could cause some issues with increased renewal processing demands due to renewal periods less than the standard. However, over time this should save money as alignment and efficiency occur.

Future Research

Based on the results of this research, the research team recommends a full cost-benefit analysis regarding the consolidation of the credentials named above. This information is imperative in order to fully understand the effect of changing the system to reflect consolidation. Furthermore, this information can provide an avenue of comparison for consolidation of the credentials versus a consolidation of the background investigation processes.

The research team also recommends a separate effort to focus entirely on consolidation of the background checks (the entire vetting process) for all credentials specific to transportation of hazardous materials. This appears to be a beneficial middle ground that provides the most benefits for the greatest number of stakeholders. This evaluation should carefully consider which credentials are viable options and which credentials are peripheral in nature. This research could result in intermediate change providing a real, positive impact to stakeholders while progressing toward an ultimate solution, should one exist.

Although it is feasible to consolidate some credentials based on currently available data, an effort needs to be implemented at the federal level with input from stakeholders at all levels. The most important next step is to identify the specific cost data associated with the security credential consolidation process.

References

1. http://digital.library.unt.edu/ark:/67531/metacrs10515/. (As of April 6, 2010.)
2. Robert N. Goldenkoff, Robert E. White, Richard Ascarate, Nikki Clowers, Cindy Gilbert, David Hooper, Tracey King, Gary Malavenda, Jean Orland, and Meg Ullengren. *Transportation Security DHS Efforts to Eliminate Redundant Background Check Investigations: Report to Congressional Committees.* U.S. Government Accountability Office, Washington, D.C. (2007).
3. http://books.nap.edu/openbook.php?record_id=11198&page=11. (As of January 22, 2008.)
4. http://www.truckline.com/Newsroom/ATA%20Comments%20Filed/ATA%20R3%20TWIC%20Petition.pdf. (As of July 21, 2009.)
5. http://www.joc.com/node/409517. (As of July 22, 2009.)
6. Dunn, W. D., *Public Policy Analysis: An Introduction* (2nd ed.), Prentice-Hall, Inc., Englewood Cliffs, NJ (1994) 480 pp.
7. Lloyd, M., *The Passport: The History of Man's Most Travelled Document*. Sutton Publishing, Stroud, U.K. (2005) 288 pp.
8. http://www.fmcsa.dot.gov/registration-licensing/cdl/cdl.htm. (As of November 3, 2010.)
9. http://managementmi.lettercarriernetwork.info/p530042.pdf. (As of June 7, 2010.)
10. http://www.cbp.gov/xp/cgov/trade/trade_outreach/advance_info/brasstrade_enforce.xml. (As of November 3, 2010.)
11. http://www.tsa.gov/press/happenings/sida.shtm. (As of October 17, 2010.)
12. Consolidation of Merchant Mariner Qualification Credentials; Final Rule, 74 Fed. Reg. 11196 (2009).
13. Transportation Worker Identification Credential (TWIC) Implementation in the Maritime Sector; Hazardous Materials Endorsement for a Commercial Driver's License, 73 Fed. Reg. 25562 (2008).
14. "Security Threat Assessment for Individuals Applying for a Hazardous Materials Endorsement for a Commercial Driver's License; Final Rule." 69 Fed. Reg. 68720 (2004).
15. http://www.tsa.gov/what_we_do/layers/twic/twic_faqs.shtm#disqualification. (As of June 2, 2010.)
16. Applicant Information Required for TWIC Security Threat Assessment, 49 C.F.R. §1572.17 (2009).
17. Applicant Responsibilities for a TWIC Security Threat Assessment, 49 C.F.R. §1572.19 (2009).
18. Disqualifying Criminal Offenses, 49 C.F.R. §1572.103 (2009).
19. http://www.tsa.gov/what_we_do/layers/twic/twic_faqs.shtm#disqualification. (As of June 2, 2010.)
20. Creditable Service and Equivalents for Licensing Purposes, 46 C.F.R. §10.211 (2009).
21. Limitation on Issuance of HazMat License, 49 U.S.C. §5103(g)
22. http://www.tsa.gov/what_we_do/layers/hazmat/disqualifiers.shtm. (As of April 28, 2010.)
23. http://www.cbp.gov/xp/cgov/trade/cargo_security/ctpat/fast/fast_driver/canada_fast_driver/fast_eligibility.xml. (As of June 2, 2010.)
24. http://www.cbp.gov/xp/cgov/travel/trusted_traveler/nexus_prog/nexus_eligibility.xml. (As of June 2, 2010.)
25. http://www.cbp.gov/xp/cgov/travel/trusted_traveler/sentri/sentri.xml. (As of June 2, 2010.)
26. Fingerprint-based Criminal History Records Check (CHRC), 49 C.F.R. §1542.209(d)
27. Denial and Restrictions of Passports, 22 C.F.R. §51.60 (2010).
28. Denial of Passports to Certain Convicted Drug Traffickers, 22 C.F.R. §51.61 (2010).
29. http://www.tsa.gov/what_we_do/layers/twic/index.shtm (As of June 6, 2010.)
30. http://www.secureidnews.com/audio/iab_0308/iab_0308_lockwood.pdf (As of June 1, 2010.)
31. http://epic.org/privacy/surveillance/spotlight/0706/pp0506.pdf. (As of June 1, 2010.)
32. http://www.tsa.gov/what_we_do/layers/hazmat/index.shtm. (As of June 6, 2010.)
33. http://www.uscg.mil/nmc/cfr.asp. (As of June 7, 2010.)
34. http://www.uscg.mil/nmc/announcements/MMC_Terminology_Information_Bulletin.pdf. (As of June 6, 2010.)
35. http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_sida_sw.pdf. (As of June 6, 2010.)
36. http://www.cbp.gov/xp/cgov/travel/trusted_traveler. (As of June 6, 2010.)
37. http://www.cbp.gov/xp/cgov/travel/trusted_traveler/nexus_prog/. (As of June 7, 2010.)
38. http://www.cbp.gov/linkhandler/cgov/newsroom/fact_sheets/travel/sentri/sentri_fact.ctt/sentri_fact.pdf. (As of June 7, 2010.)
39. http://managementmi.lettercarriernetwork.info/p530042.pdf. (As of June 7, 2010.)
40. http://travel.state.gov/passport/ppi/ppi_4856.html. (As of June 7, 2010.)
41. http://travel.state.gov/travel/cbpmc/cbpmc_2223.html. (As of June 7, 2010.)

42. http://www.cac.mil. (As of June 7, 2010.)
43. http://www.fema.gov/good_guidance/download/10280. (As of May 6, 2010.)
44. Jensen, J. L., "A Multipopulation Comparison of the Diffusion of Public Organizations and Policies across Time and Space." *Policy Studies Journal,* Vol. 32, No. 1, ABI/INFORM Global (2004) pp. 109–127.
45. Waldron, M., "Overcoming Barriers to Change in Management Accounting Systems." *Journal of American Academy of Business, Cambridge,* Vol. 6, No. 2, ABI/INFORM Global (2005) pp. 244–249.
46. Hazardous Materials Program Definitions and General Procedures, 49 C.F.R. pt. 105 (2007).
47. http://www.dhs.gov/xabout/laws/gc_1217616624097.shtm#1. (As of December 29, 2010.)
48. United States Department of Commerce, *Personal Identity Verification (PIV) of Federal Employees and Contractors* (FIPS PUB 201-1). National Institute of Standards and Technology, Gaithersburg, MD (2006).

List of Acronyms

3-D—Three-dimensional
AAAE—American Association of Airport Executives
AB—Able Seaman
ATF—Bureau of Alcohol, Tobacco, Firearms and Explosives
CA—Bureau of Consular Affairs
CAC—Common Access Card
CBP—Customs and Border Protection
CDL—Commercial Driver's License
CDL-HME—Commercial Driver's License—Hazardous Materials Endorsement
CEO—Chief Executive Officer
CFR—Code of Federal Regulations
CMV—Commercial Motor Vehicle
CMVSA—Commercial Motor Vehicle Safety Act of 1986
COR—Certificate of Registry
CPPI—Canadian Petroleum Products Institute
DEERS—Defense Enrollment Eligibility Reporting System
FAST—Free and Secure Trade
FBI—Federal Bureau of Investigation
FELA—Federal Employer's Liability Act
FIPS—Federal Information Processing Standards
FUPAC—Florida Uniform Port Access Credential
GRT—Gross Register Tonnage
HazMat—Hazardous Materials
HME—Hazardous Materials Endorsement
HSPD-12—Homeland Security Presidential Directive 12
IAD—Washington Dulles International Airport
ICC—Integrated Circuit Chip
ID—Identification
IMO—International Maritime Organization
MMC—Merchant Mariner Credential
MMD—Merchant Mariner Document
MML—Merchant Mariner License

MTSA—Maritime Transportation Security Act
NACI—National Agency Check with Inquiries
NCIC—National Crime Information Center
NIST—National Institute of Standards and Technology
PIV—Personal Identity Verification
PIV-I—Personal Identity Verification Interoperability
RFID—Radio Frequency Identification
RICO—Racketeer Influenced and Corrupt Organizations
SAFE—Security and Accountability for Every Port Act of 2006
SBA—Small Business Administration
SENTRI—Secure Electronic Network for Travelers Rapid Inspection
SIDA—Security Identification Display Area
STCW—Standards of Training, Certification, and Watchkeeping for Seafarers
SWOT—Strengths, Weaknesses, Opportunities, and Threats
TAG—Technical Advisory Group
TSA—Transportation Security Administration
TWIC—Transportation Worker Identification Credential
USA PATRIOT Act—Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001
U.S.C.—United States Code
USCG—United States Coast Guard
USPS—United States Postal Service
U/V—Ultraviolet
VTA—Virginia Trucking Association
VTTI—Virginia Tech Transportation Institute
WHTI—Western Hemisphere Travel Initiative

APPENDIX A

Technical Advisory Group Biographies

Karen Chappell

Ms. Chappell is the former Deputy Commissioner of the Virginia Department of Motor Vehicles. Among her other responsibilities, Ms. Chappell oversaw the CDL with HazMat endorsement process. Furthermore, Ms. Chappell was involved in a Virginia study of credentialing processes. Ms. Chappell was asked to join the TAG based on her experience in evaluating and changing the credentialing process, in addition to her knowledge of the state credentialing system.

Wiley Mitchell

Mr. Mitchell is the former senior general counsel of Norfolk Southern Railroad and currently serves as special counsel. Mr. Mitchell was responsible for casualty claims and litigation, the Federal Employers Liability Act (FELA) and insurance litigation at Norfolk Southern. Mr. Mitchell is a member of the firm's government relations practice group, specializing in state and local government issues. In addition, he is engaged in rail transportation law with Willcox & Savage in Norfolk. Mr. Mitchell is a past national president and a current member of the executive committee of the National Association of Railroad Trial Counsel. He is the immediate past chair of the Virginia Rail Advisory Committee and Vice Chair of the Virginia Rail Policy Institute. Mr. Mitchell was asked to participate because of his expansive knowledge of freight rail issues especially related to employee credentialing.

Dr. Walter Witschey

Dr. Witschey has more than 40 years of experience in business management in both the public and private sectors. He served 14 years as president and CEO of a computer services business and has an extensive background as an independent business and systems management consultant. From 1992 until 2007 he served as the director of the Science Museum of Virginia, a large state-agency, multi-site science center network. He is past president of the Association of Science-Technology Centers and past president of the Virginia Academy of Science. Dr. Witschey is currently the Chairman of the Virginia Rail Policy Institute and was asked to participate because of his extensive contacts with individuals who have knowledge of transportation-related issues, as well as his science and technology expertise.

Jim Wilding

Mr. Wilding is the retired president and CEO of the Metropolitan Washington Airports Authority. Mr. Wilding's aviation career spans 43 years. He is a graduate civil engineer with prior service with the FAA. Mr. Wilding held progressively responsible positions in all phases of engineering for the two federally owned airports, Washington Dulles International and Ronald Reagan Washington National, eventually becoming the organization's chief engineer. He served as chief engineer until becoming the airports' deputy director in 1975 and as director 4 years later. Mr. Wilding was asked to participate to represent the interests of a major airport, as well as for his extremely broad contacts and expertise in aviation matters, including freight issues.

John Smith

Mr. Smith is the vice president of Shenandoah Logistics. He is currently the executive director of the Virginia Rail Policy Institute. Mr. Smith gained experience in trucking and shipping as director of operations for VHI Transport and as operations manager for the Port of Richmond. Mr. Smith has had direct experience with the credentialing process, including applying for, and obtaining, the TWIC. Mr. Smith was asked to participate as a representative of trucking-logistics concerns and for his experience in the credentialing process and procedures from the perspective of the trucking industry.

Lt. Sal Castruita

Lt. Castruita is an Operations Division lieutenant for the Virginia Port Authority Police Department. He oversees the law enforcement operations of two marine terminals in the Hampton Roads area: the Portsmouth Marine Terminal and the Newport News Marine Terminal. He has extensive experience and responsibility for the proper credentialing of those persons who wish to access the port facility. He has direct experience with proper display, currency, and validation of credentials. He was asked to participate because of his knowledge of port operations, enforcement, and security related to the credentialing process.

Dale Bennett

Mr. Bennett is the president and CEO of the Virginia Trucking Association (VTA). As the executive head of the VTA, Mr. Bennett has immediate and extensive access to trucking companies, private fleet operators, industry suppliers, and other firms and individuals interested in the well being of motor freight transportation at the local, state, and national levels. Mr. Bennett was asked to participate because he can provide direct access to persons who may have valuable information about the credentialing process and its use.

APPENDIX B

Requirements to Obtain

Table B-1. Singularly applicable requirements to obtain.

Credential	Applicable Mode	Race	Additional Contact Phone Numbers	Emergency Contact Information	Father's Citizenship	Father's Date of Birth	Father's Name	Father's Place of Birth	Marriage Status (Data)	Mother's Citizenship	Mother's Date of Birth	Mother's Name	Mother's Place of Birth	Previous Credential Data	Travel Plans	Employer Fax #	Preferred Notification Method	Drug Testing	Next of Kin Email Address	Next of Kin Phone Number	Certification of Qualification	Drivers Licensing History	Former Names	Related Medical History	Selective Service Status	Company Registration	Residence	Copy of Drivers License	Education (History)	Military Service	Screening by Agency/Other Federal Agencies in last year	Drivers License Number	Age	Interview with CBP officer	Sponsoring Agency Information
SIDA	Air	●																																	
Passport	All		●	●	●	●	●	●	●	●	●	●	●	●	●																				
TWIC	Marine															●	●																		
MMD	Marine																	●	●	●															
MMC	Marine																	●																	
CDL-HME	Highway																				●	●	●	●	●										
FAST	Highway																									●	●								
USPS	Highway																											●	●	●	●				
NEXUS	Highway																															●			
SENTRI	Highway																																●	●	
CAC	Highway																																		●

APPENDIX C

Disqualifying Offenses Table

Table C-1. Disqualifying offenses, Part 1.

1 to 30	Disqualifying Offenses	TWIC	CDL-HME	MMD	MML	MMC	FAST	SIDA	Passport	NEXUS	SENTRI	e-RailSafe	CAC*	USPS
1	A crime involving a transportation security incident	●	●											
2	A crime listed in 18 U.S.C. Chapter 113B—Terrorism, or a state law that is comparable	●	●											
3	Aggravated assault			●	●	●		●						
4	Aircraft piracy							●						
5	Aircraft piracy outside the special aircraft jurisdiction of the United States							●						
6	Arson	●	●					●						
7	Assault with Intent to murder	●	●					●						
8	Bribery	●	●					●						
9	Burglary			●	●	●		●						
10	Cannot satisfy CBP of their low-risk status (i.e., CBP has intelligence that indicates that the applicant is not low risk; CBP cannot determine an applicant's criminal, residence or employment history)										●			
11	Carrying a Weapon or explosive aboard aircraft							●						
12	Commission of certain crimes aboard aircraft in flight							●						
13	Conspiracy	●	●					●						
14	Conspiracy or attempt to commit any of these crimes	●	●											
15	Conveying false information and threats							●						
16	Convicted of a criminal offense						●			●				
17	Conviction involving a fatality (vehicular crime)			●	●	●								
18	Criminal violations of environmental laws			●	●	●								
19	Criminal violations of environmental laws involving pollutants or HazMat			●	●	●								
20	Destruction of aircraft or aircraft facility							●						
21	Dishonesty, fraud, or misrepresentation, including identity fraud	●	●					●						
22	Distribution, possession with intent to distribute, or importation of a controlled substance, including drugs	●	●	●	●	●		●						●
23	Espionage	●	●					●						
24	Extortion	●	●					●						
25	Felony involving a threat							●						
26	Forgery of certificates, false markings of aircraft, and other aircraft registration violations							●						
27	Homicide (unintentional)			●	●	●								
28	Illegal possession of a controlled substance punishable by a maximum term of imprisonment of more than 1 year.			●	●	●		●	●					●
29	Immigration Violations	●	●											
30	Importation or manufacture of a controlled substance							●	●					●

*Unable to verify the disqualifying offenses for the Common Access Card.

Table C-2. Disqualifying offenses, Part 2.

31 to 60	Disqualifying Offenses	TWIC	CDL-HME	MMD	MML	MMC	FAST	SIDA	Passport	NEXUS	SENTRI	e-RailSafe	CAC*	USPS
31	Imprisonment > 1 Year	●												
32	Improper transportation of Hazardous Materials under 49 U.S.C. 5124 or a state law that is comparable	●	●					●						
33	Inadmissible to the United States under immigration regulation, including applicants with approved waivers of inadmissibility or parole documentation									●	●			
34	Interference with air navigation							●						
35	Interference with flight crew members or flight attendants							●						
36	Kidnapping or hostage taking	●	●					●						
37	Lesser RICO violations	●	●											
38	Lighting violations involving transporting controlled substances							●						
39	Murder	●	●	●	●	●		●						
40	Pending criminal charges										●			
41	Possession or distribution of stolen property							●						
42	Racing on the highways			●	●	●								
43	Rape or aggravated sexual abuse	●	●	●	●	●		●						
44	Reckless driving			●	●	●								
45	Robbery	●	●	●	●	●		●						
46	Sedition	●	●					●						
47	Simple assault			●	●	●								
48	Smuggling	●	●											
49	Subject of an ongoing investigation by any federal, state, or local law enforcement agency										●			
50	Subject to National Security Entry Exit Registration System (NSEERS) or other special registration programs										●			
51	Theft (embezzlement)			●	●	●		●						
52	Treason	●	●					●						
53	Unlawful entry into an aircraft or airport area that serves air carriers or foreign air carriers contrary to established security requirements							●						
54	Unlawful possession, use, sale, distribution, manufacture, purchase, receipt, transfer, shipping, transporting, import, export, storage of, or dealing in an explosive or explosive device	●	●											
55	Unlawful possession, use, sale, distribution, manufacture, purchase, receipt, transfer, shipping, transporting, import, export, storage of, or dealing in a firearm or other weapons	●	●					●						
56	Violation of any customs, immigration or agriculture regulations or laws in any country									●	●			
57	Violations of the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. 1961, et seq., or a state law that is comparable, where one of the predicate acts found by a jury or admitted by the defendant, consists of one of the offenses listed in paragraphs (d) or (h) of this section	●	●											
58	Violence at international airports							●						
59	Will not lawfully reside in either Canada or the United States for term of credential									●				
60	Willful destruction of property			●	●	●		●						

Table C-3. Disqualifying offenses, Part 3.

61 to 93	Disqualifying Offenses	TWIC	CDL-HME	MMD	MML	MMC	FAST	SIDA	Passport	NEXUS	SENTRI	e-RailSafe	CAC*	USPS
61	U.S. loan default 22 CFR 51.60								●					
62	Arrears of child support 42 U.S.C. 2671(b)(2)(B)								●					
63	Outstanding federal warrant or arrest for felony 18 U.S.C. 1073								●					●
64	Subject to criminal court order, condition of probation, or condition of parole, any of which forbid departure from the United States								●					
65	Subject to court order committing one to a mental institution								●					
66	Declared legally incompetent	●							●					
67	Subject of request for extradition								●					
68	Subject of a subpoena received from the United States pursuant to 28 U.S.C. 1783								●					
69	Applicant is minor, and passport may be denied under 22 CFR 51.28								●					
70	Subject to an order of restraint or apprehension issued by an appropriate officer of the U.S. Armed Forces under Ch.47, Title 10 U.S.C.								●					
71	Subject to an outstanding state or local warrant of arrest for a felony								●					●
72	Subject of a request for extradition or provisional arrest submitted to the United States by a foreign country								●					
73	Previously denied the credential								●					
74	Threat to national security or foreign policy								●					
75	Minor applicant involved in custody battle								●					
76	Trafficking								●					
77	Conviction of a felony offense in the last 7 years											●		●
78	Released from a penal institution in the last 5 years											●		
79	Active misdemeanor and felony warrants											●		
80	Any pending felony charge											●		●
81	Social Security fraud alerts											●		
82	A history of crimes of concern											●		
83	Out of service area											●		
84	Permanent disqualifier											●		
85	Background check canceled by contractor											●		
86	Convicted of offenses involving dishonesty													●
87	Convicted of offenses involving moral turpitude													●
88	Convicted of offenses involving financial gain													●
89	On parole, probation, or under suspended sentence for commision of a felony													●
90	On parole, probation, or under suspended sentence for any controlled substance charge													●
91	Pending controlled substance charges													●
92	Pattern of criminal conduct													●
93	Conviction, investigation of, or under indictment for stealing mail or other postal crimes													●

APPENDIX D

Credential-Specific Survey Response Data

Table D-1. Data collection process progress summary.

Date	Week #	Total Responses	Air	Highway/Tractor-Trailer	Marine	Rail	Mode Unknown
28-Apr-10	1	8	1	4	0	0	3
5-May-10	2	46	4	25	25	11	5
12-May-10	3	53	7	30	29	14	5
19-May-10	4	63	10	39	34	16	5
26-May-10	5	69	10	43	34	18	5
2-Jun-10	6	156	13	128	38	26	7
9-Jun-10	7	293	20	261	41	30	9
16-Jun-10	8	346	20	313	42	30	10
23-Jun-10	9	362	21	329	43	31	10
30-Jun-10	10	378	21	345	43	31	10
Total		378	21	345	43	31	10

Table D-2. Respondents' total time to obtain a credential, from beginning of application process through receipt of credential.

	Less than 2 weeks	2 to 4 weeks	5 to 8 weeks	9 to 12 weeks	13 to 16 weeks	Greater than 16 weeks	Total
CDL-HME	57 (21.0%)	109 (40.1%)	74 (27.2%)	20 (7.4%)	7 (2.6%)	5 (1.8%)	272 (100%)
TWIC	12 (5.4%)	76 (33.9%)	81 (36.2%)	27 (12.1%)	12 (5.4%)	16 (7.1%)	224 (100%)
FAST	2 (9.1%)	5 (22.7%)	6 (27.3%)	3 (13.6%)	2 (9.1%)	4 (18.2%)	22 (100%)
FUPAC	5 (62.5%)	3 (37.5%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	8 (100%)
MMC	0 (0%)	1 (20.0%)	1 (20.0%)	0 (0%)	2 (40%)	1 (20%)	5 (100%)
MMD	0 (0%)	0 (0%)	1 (25.0%)	0 (0%)	2 (50.0%)	1 (25.0%)	4 (100%)
MML	1 (25.0%)	0 (0%)	1 (25.0%)	0 (0%)	1 (25.0%)	1 (25.0%)	4 (100%)
SENTRI	1 (50.0%)	0 (0%)	1 (50.0%)	0 (0%)	0 (0%)	0 (0%)	2 (100%)
SIDA	3 (60.0%)	1 (20.0%)	1 (20.0%)	0 (0%)	0 (0%)	0 (0%)	5 (100%)
Other	25 (45.5%)	12 (21.8%)	11 (20.0%)	4 (7.3%)	0 (0%)	3 (5.5%)	55 (100%)
Total	106	207	177	54	26	31	601
Percent	17.6%	34.4%	29.5%	9.0%	3.7%	5.2%	100%

Note: Due to rounding, the totals may not add up to 100%.

Table D-3. Respondents' perception of the total time needed to obtain a credential, from beginning of application process through receipt of credential.

	Way Too Short	Too Short	About Right	Too Long	Way Too Long	Total
CDL-HME	0 (0%)	4 (1.5%)	124 (46.1%)	103 (38.3%)	38 (14.1%)	269 (100%)
TWIC	1 (0.4%)	0 (0%)	60 (26.8%)	101 (45.1%)	62 (27.7%)	224 (100%)
FAST	0 (0%)	0 (0%)	6 (27.3%)	8 (36.4%)	8 (36.4%)	22 (100%)
FUPAC	0 (0%)	0 (0%)	3 (37.5%)	5 (62.5%)	0 (0%)	8 (100%)
MMC	0 (0%)	0 (0%)	3 (60%)	0 (0%)	2 (40%)	5 (100%)
MMD	0 (0%)	0 (0%)	1 (25.0%)	1 (25.0%)	2 (50.0%)	4 (100%)
MML	0 (0%)	0 (0%)	2 (50.0%)	1 (25.0%)	1 (25.0%)	4 (100%)
SENTRI	0 (0%)	0 (0%)	1 (50.0%)	1 (50.0%)	0 (0%)	2 (100%)
SIDA	0 (0%)	0 (0%)	5 (100.0%)	0 (0%)	0 (0%)	5 (100%)
Other	0 (0%)	1 (1.8%)	33 (58.9%)	14 (25.0%)	8 (14.3%)	56 (100%)
Total	1	5	238	234	121	599
Percent	0.2%	0.8%	39.7%	39.1%	20.2%	100%

Note: Due to rounding, the totals may not add up to 100%.

Table D-4. Respondents' time to complete the application process.

	Less than 2 hours	2 to 4 hours	5 to 8 hours	9 to 16 hours	Greater than 16 hours	Total
CDL-HME	177 (66.3%)	71 (26.6%)	14 (5.2%)	2 (0.7%)	3 (1.1%)	267 (99.9%)
TWIC	134 (61.2%)	71 (32.4%)	12 (5.5%)	2 (0.9%)	0 (0%)	219 (100%)
FAST	13 (59.1%)	8 (36.4%)	1 (4.5%)	0 (0%)	0 (0%)	22 (100%)
FUPAC	6 (85.7%)	1 (14.3%)	0 (0%)	0 (0%)	0 (0%)	7 (100%)
MMC	4 (80%)	1 (20%)	0 (0%)	0 (0%)	0 (0%)	5 (100%)
MMD	2 (50.0%)	0 (0%)	2 (50.0%)	0 (0%)	0 (0%)	4 (100%)
MML	3 (75.0%)	0 (0%)	0 (0%)	1 (25.0%)	0 (0%)	4 (100%)
SENTRI	0 (0%)	2 (100.0%)	0 (0%)	0 (0%)	0 (0%)	2 (100%)
SIDA	3 (60.0%)	1 (20.0%)	0 (0%)	0 (0%)	1 (20.0%)	5 (100%)
Other	19 (52.8%)	9 (25.0%)	5 (13.9%)	0 (0%)	3 (8.3%)	36 (100%)
Total	361	164	34	5	7	571
Percent	63.2%	28.7%	6.0%	0.9%	1.2%	100%

Note: Due to rounding, the totals may not add up to 100%.

Table D-5. Respondents' perception of the time to complete the application process.

	Way Too Short	Too Short	About Right	Too Long	Way Too Long	Total
CDL-HME	1 (0.4%)	2 (0.8%)	197 (74.1%)	54 (20.3%)	12 (4.5%)	266 (100%)
TWIC	0 (0%)	0 (0%)	132 (60.3%)	68 (31.1%)	19 (8.7%)	219 (100%)
FAST	0 (0%)	0 (0%)	16 (72.7%)	4 (18.2%)	2 (9.1%)	22 (100%)
FUPAC	0 (0%)	0 (0%)	3 (37.5%)	5 (62.5%)	0 (0%)	8 (100%)
MMC	0 (0%)	0 (0%)	40 (80%)	1 (20%)	0 (0%)	5 (100%)
MMD	0 (0%)	0 (0%)	3 (75.0%)	0 (0%)	1 (25.0%)	4 (100%)
MML	0 (0%)	0 (0%)	3 (75.0%)	1 (25.0%)	0 (0%)	4 (100%)
SENTRI	0 (0%)	0 (0%)	2 (100.0%)	0 (0%)	0 (0%)	2 (100%)
SIDA	0 (0%)	0 (0%)	5 (100.0%)	0 (0%)	0 (0%)	5 (100%)
Other	0 (0%)	1 (1.9%)	40 (74.1%)	10 (18.5%)	3 (5.6%)	54 (100%)
Total	1	3	441	143	37	589
Percent	0.2%	0.5%	74.9%	24.3%	6.3%	100%

Note: Due to rounding, the totals may not add up to 100%.

Table D-6. Respondents' total travel time to obtain the credential once ready for pick up.

	Less than 2 hours	2 to 4 hours	5 to 8 hours	9 to 16 hours	Greater than 16 hours	Total
CDL-HME	220 (83.3%)	35 (13.3%)	7 (2.7%)	1 (0.4%)	1 (0.4%)	264 (100%)
TWIC	158 (72.1%)	40 (18.3%)	16 (7.3%)	3 (1.4%)	2 (0.9%)	219 (100%)
FAST	7 (31.8%)	6 (27.3%)	5 (22.7%)	2 (9.1%)	2 (9.1%)	22 (100%)
FUPAC	6 (75%)	0 (0%)	1 (12.5%)	0 (0%)	1 (12.5%)	8 (100%)
MMC	3 (60.0%)	1 (20%)	1 (20%)	0 (0%)	0 (0%)	5 (100%)
MMD	2 (50.0%)	1 (25.0%)	1 (25.0%)	0 (0%)	0 (0%)	4 (100%)
MML	2 (50.0%)	1 (25.0%)	1 (25.0%)	0 (0%)	0 (0%)	4 (100%)
SENTRI	1 (50.0%)	1 (50.0%)	0 (0%)	0 (0%)	0 (0%)	2 (100%)
SIDA	4 (80.0%)	0 (0%)	1 (20.0%)	0 (0%)	0 (0%)	5 (100%)
Other	38 (70.4%)	7 (13.0%)	0 (0%)	1 (1.9%)	8 (14.8%)	54 (100%)
Total	441	92	33	7	14	587
Percent	75.1%	15.7%	5.6%	1.2%	2.4%	1000%

Note: Due to rounding, the totals may not add up to 100%.

Table D-7. Respondents' perception of the total travel time necessary to obtain the credential once ready for pick up.

	Way Too Short	Too Short	About Right	Too Long	Way Too Long	Total
CDL-HME	1 (0.4%)	1 (0.4%)	193 (73.1%)	56 (21.2%)	13 (4.9%)	264 (100%)
TWIC	2 (0.9%)	0 (0%)	117 (53.2%)	77 (35.0%)	24 (10.9%)	220 (100%)
FAST	0 (0%)	0 (0%)	8 (36.4%)	10 (45.5%)	4 (18.2%)	22 (100%)
FUPAC	0 (0%)	0 (0%)	4 (50%)	3 (37.5%)	1 (12.5%)	8 (100%)
MMC	0 (0%)	0 (0%)	3 (60.0%)	1 (20.0%)	1 (20.0%)	5 (100%)
MMD	0 (0%)	0 (0%)	2 (50.0%)	0 (0%)	2 (50.0%)	4 (100%)
MML	0 (0%)	0 (0%)	2 (50.0%)	2 (50.0%)	0 (0%)	4 (100%)
SENTRI	0 (0%)	0 (0%)	1 (100.0%)	0 (0%)	0 (0%)	1 (100%)
SIDA	0 (0%)	1 (20.0%)	4 (80.0%)	0 (0%)	0 (0%)	5 (100%)
Other	0 (0%)	0 (0%)	44 (81.5%)	8 (14.8%)	2 (3.7%)	54 (100%)
Total	3	2	378	157	47	587
Percent	0.5%	0.3%	64.4%	26.7%	8.0%	100%

Cross-Tabulated Data

Table D-8. Total time to obtain credential and perceptions.

	Less than 2 weeks	2 to 4 weeks	5 to 8 weeks	9 to 12 weeks	13 to 16 weeks	Greater than 16 weeks	Total
CDL-HME							
Too Long	6	45	38	10	4	0	103
Way Too Long	1	9	14	7	3	4	38
TWIC							
Too Long	1	32	50	12	3	3	101
Way Too Long	1	9	18	13	8	13	62
FAST							
Too Long	1	1	3	2	1	0	8
Way Too Long	0	0	2	1	1	5	9
FUPAC							
Too Long	3	2	0	0	0	0	5
Way Too Long	0	0	0	0	0	0	0
MMC							
Too Long	0	0	0	0	0	0	0
Way Too Long	0	0	0	0	1	1	2
MMD							
Too Long	0	0	1	0	0	0	1
Way Too Long	0	0	0	0	1	1	2
MML							
Too Long	0	0	0	0	1	0	1
Way Too Long	0	0	0	0	0	1	1
SENTRI							
Too Long	0	0	1	0	0	0	1
Way Too Long	0	0	0	0	0	0	0
SIDA							
Too Long	0	0	0	0	0	0	0
Way Too Long	0	0	0	0	0	0	0
OTHER							
Too Long	2	5	5	1	0	0	13
Way Too Long	0	0	3	2	0	2	7
Grand Totals							
Too Long	13	85	98	25	9	3	233
Way Too Long	2	18	37	23	14	27	121

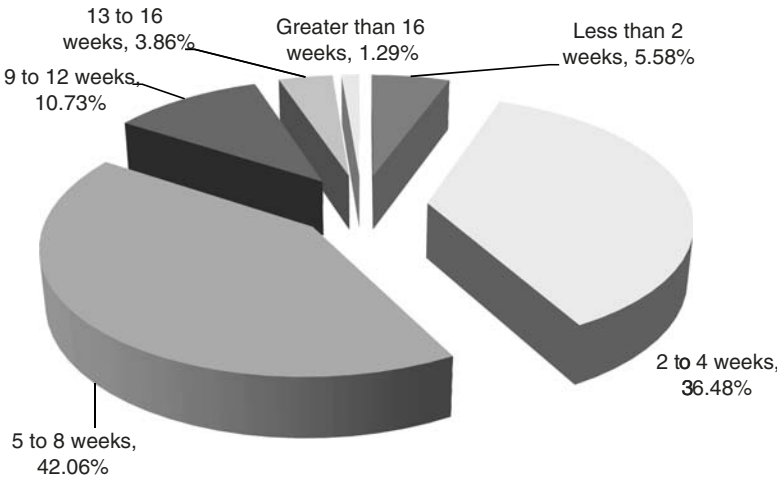

Figure D-1. Percentage of respondents indicating that the total time to obtain the credential was too long.

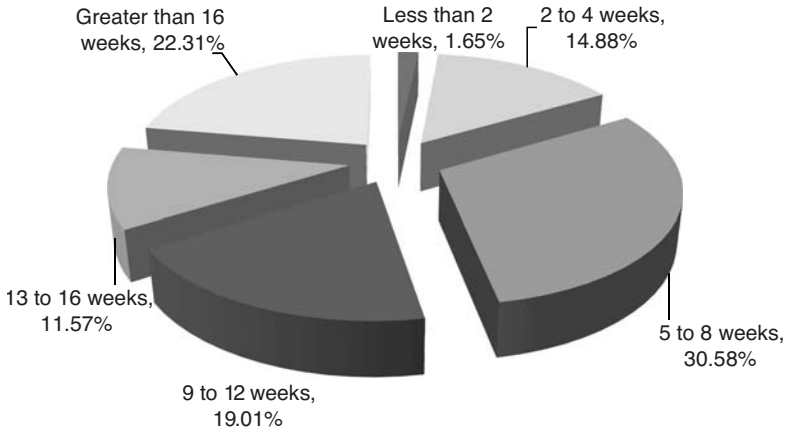

Figure D-2. Percentage of respondents indicating that the total time to obtain the credential was way too long.

Table D-9. Time to complete credential application and perceptions.

	Less than 2 hours	2 to 4 hours	5 to 8 hours	9 to 12 hours	Greater than 16 hours	Total
CDL-HME						
Too Long	18	28	8	0	0	**54**
Way Too Long	2	4	3	1	2	**12**
TWIC						
Too Long	18	44	5	0	0	**67**
Way Too Long	4	9	5	1	0	**19**
FAST						
Too Long	0	3	1	0	0	**4**
Way Too Long	0	2	0	0	0	**2**
FUPAC						
Too Long	4	1	0	0	0	**5**
Way Too Long	0	0	0	0	0	**0**
MMC						
Too Long	0	1	0	0	0	**1**
Way Too Long	0	0	0	0	0	**0**
MMD						
Too Long	0	0	1	0	0	**1**
Way Too Long	0	0	0	0	0	**0**
MML						
Too Long	0	0	0	1	0	**1**
Way Too Long	0	0	0	0	0	**0**
SENTRI						
Too Long	0	0	0	0	0	**0**
Way Too Long	0	0	0	0	0	**0**
SIDA						
Too Long	0	0	0	0	0	**0**
Way Too Long	0	0	0	0	0	**0**
OTHER						
Too Long	2	3	3	0	0	**8**
Way Too Long	0	0	2	0	1	**3**
Grand Totals						
Too Long	42	80	18	1	0	141
Way Too Long	6	15	10	2	3	36

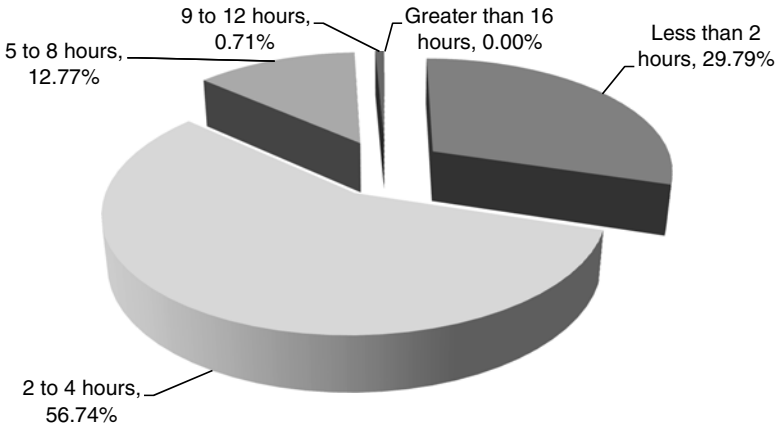

Figure D-3. Percentage of respondents indicating that the total time to complete credential application was too long.

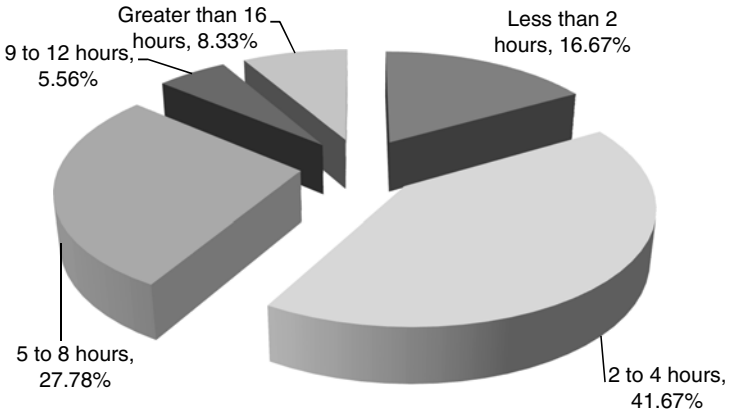

Figure D-4. Percentage of respondents indicating that the total time to complete credential application was way too long.

Table D-10. Total time to pick up credential and perceptions.

	Less than 2 hours	2 to 4 hours	5 to 8 hours	9 to 12 hours	Greater than 16 hours	Total
CDL-HME						
Too Long	34	18	4	0	0	**56**
Way Too Long	2	8	1	1	1	**13**
TWIC						
Too Long	46	26	4	0	0	**77**
Way Too Long	6	7	9	0	1	**23**
FAST						
Too Long	3	2	2	2	1	**10**
Way Too Long	0	0	3	0	1	**4**
FUPAC						
Too Long	2	0	1	0	0	**3**
Way Too Long	0	0	0	0	1	**1**
MMC						
Too Long	0	1	0	0	0	**1**
Way Too Long	0	0	1	0	0	**1**
MMD						
Too Long	0	0	0	0	0	**0**
Way Too Long	0	1	1	0	0	**2**
MML						
Too Long	0	1	1	0	0	**2**
Way Too Long	0	0	0	0	0	**0**
SENTRI						
Too Long	0	0	0	0	0	**0**
Way Too Long	0	0	0	0	0	**0**
SIDA						
Too Long	0	0	0	0	0	**0**
Way Too Long	0	0	0	0	0	**0**
OTHER						
Too Long	2	2	0	1	3	**8**
Way Too Long	0	0	0	0	2	**2**
Grand Totals						
Too Long	**87**	**50**	**12**	**3**	**4**	**157**
Way Too Long	**8**	**16**	**15**	**1**	**6**	**46**

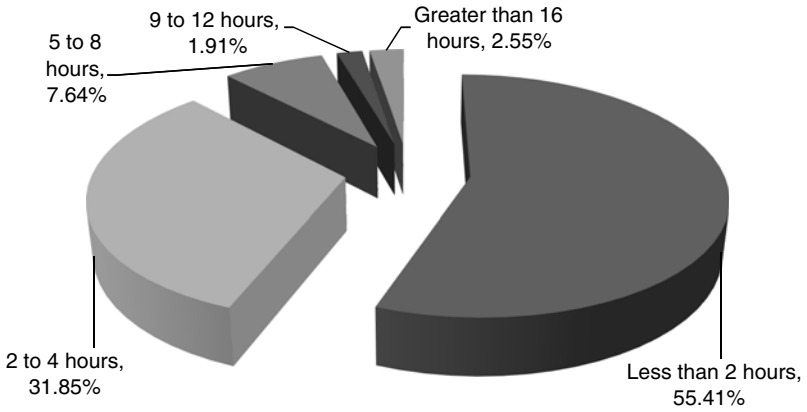

Figure D-5. Percentage of respondents indicating that the travel time to pick up the credential application was too long.

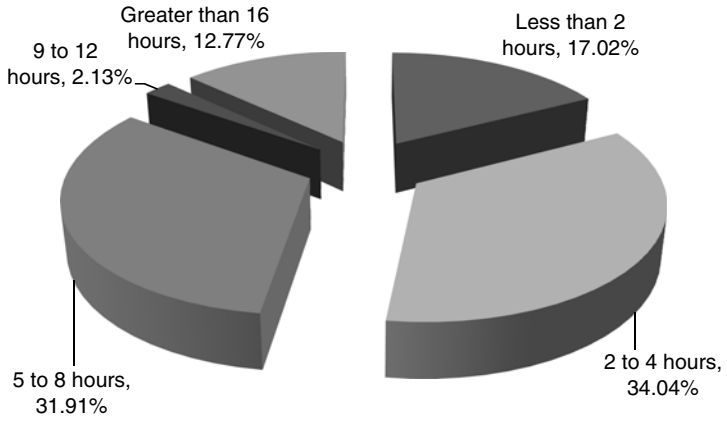

Figure D-6. Percentage of respondents indicating that the travel time to pick up the credential was way too long.

APPENDIX E

CDL-HME and Threat Assessment Costs by State

Table E-1. CDL-HME costs.

State (Issuing Entity)	CDL-HME	Renewal	Threat Assessment	Renewal
Alabama	$ 53.50	$ 53.50	$ 89.25	$ 89.25
Alaska	$ 100.00	$ 100.00	$ 89.25	$ 89.25
Arizona	$ 35.00	$ 25.00	$ 89.25	$ 89.25
Arkansas	$ 42.00	$ 42.00	$ 89.25	$ 89.25
California	$ 100.00	$ 39.00	$ 89.25	$ 89.25
Colorado	$ 35.00	$ 35.00	$ 89.25	$ 89.25
Connecticut	$ 80.00	$ 60.00	$ 89.25	$ 89.25
Delaware	$ 35.00	$ 35.00	$ 89.25	$ 89.25
District of Columbia	$ 117.00	$ 117.00	$ 89.25	$ 89.25
Florida	$ 82.00	$ 82.00	$ 91.00	$ 91.00
Georgia	$ 35.00	$ 35.00	$ 89.25	$ 89.25
Hawaii	$ 35.00	$ 35.00	$ 89.25	$ 89.25
Idaho	$ 55.00	$ 55.00	$ 89.25	$ 89.25
Illinois	$ 65.00	$ 65.00	$ 89.25	$ 89.25
Indiana	$ 30.00	$ 30.00	$ 89.25	$ 89.25
Iowa	$ 45.00	$ 45.00	$ 89.25	$ 89.25
Kansas	$ 36.00	$ 36.00	$ 95.00	$ 95.00
Kentucky	$ 45.00	$ 47.00	$ 115.00	$ 115.00
Louisiana	$ 59.00	$ 59.00	$ 89.25	$ 89.25
Maine	$ 44.00	$ 34.00	$ 89.25	$ 89.25
Maryland	$ 50.00	$ 50.00	$ 93.25	$ 89.25
Massachusetts	$ 85.00	$ 85.00	$ 89.25	$ 89.25
Michigan	$ 30.00	$ 30.00	$ 89.25	$ 89.25
Minnesota	$ 45.50	$ 45.50	$ 89.25	$ 89.25
Mississippi	$ 72.00	$ 72.00	$ 89.25	$ 89.25
Missouri	$ 45.00	$ 45.00	$ 89.25	$ 89.25
Montana	$ 50.50	$ 50.00	$ 89.25	$ 89.25
Nebraska	$ 57.50	$ 57.50	$ 89.25	$ 89.25
Nevada	$ 104.00	$ 87.00	$ 89.25	$ 89.25
New Hampshire	$ 70.00	$ 70.00	$ 89.25	$ 89.25
New Jersey	$ 44.00	$ 44.00	$ 89.25	$ 89.25
New Mexico	$ 34.00	$ 34.00	$ 125.00	$ 125.00
New York	$ 185.50	$ 185.50	$ 140.75	$ 140.75
North Carolina	$ 144.00	$ 144.00	$ 89.25	$ 89.25

Table E-1. (Continued).

North Dakota	$ 18.00	$ 18.00	$ 89.25	$ 89.25
Ohio	$ 43.00	$ 44.75	$ 89.25	$ 89.25
Oklahoma	$ 41.50	$ 41.50	$ 89.25	$ 89.25
Oregon	$ 145.50	$ 61.50	$ 89.25	$ 89.25
Pennsylvania	$ 88.00	$ 78.00	$ 60.00	$ 60.00
Rhode Island	$ 51.50	$ 51.50	$ 89.25	$ 89.25
South Carolina	$ 29.50	$ 29.50	$ 78.25	$ 78.25
South Dakota	$ 35.00	$ 35.00	$ 89.25	$ 89.25
Tennessee	$ 42.50	$ 42.50	$ 82.00	$ 82.00
Texas	$ 60.00	$ 60.00	$ 78.20	$ 78.20
Utah	$ 107.00	$ 107.00	$ 89.25	$ 89.25
Vermont	$ 85.00	$ 85.00	$ 89.25	$ 89.25
Virginia	$ 65.00	$ 65.00	$ 83.00	$ 83.00
Washington	$ 50.00	$ 55.00	$ 89.25	$ 89.25
West Virginia	$ 48.75	$ 48.75	$ 89.25	$ 89.25
Wisconsin	$ 79.00	$ 79.00	$ 81.25	$ 71.25
Wyoming	$ 25.00	$ 25.00	$ 89.25	$ 89.25

APPENDIX F

SIDA Badge Costs

Table F-1. SIDA badge costing based on a sampling of airports.

Airport Location	SIDA Badge Cost
Peoria, IL	$ 75.00
Atlanta, GA	$ 60.00
Anchorage, AK	$ 10.00
Bedford, MA	$ 75.00
La Crosse, WI	$ 81.00
Dallas/Fort Worth, TX	$ 100.00
Minneapolis/St. Paul, MN	$ 280.00
Asheville, NC	$ 52.00
Phoenix, AZ	$ 89.00
Mean	$ 91.33

APPENDIX G

Sample of Port Credential Requirements

Table G-1. Required port security access credentials.

	TWIC Only	TWIC and Port ID
Bridgeport, Connecticut	●	
Brunswick, Georgia		●
Camden-Gloucester City, New Jersey		●
Charleston, South Carolina	●	
Chester, Pennsylvania	●	
Georgetown, South Carolina	●	
Grays Harbor, Washington	●	
Guntersville, Alabama	●	
Helen Delich Bentley Port of Baltimore, Maryland		●
Hilo, Hawaii		●
Kalama, Washington	●	
Kawaihae, Hawaii		●
Louisville, Kentucky	●	
Marcus Hook, Pennsylvania	●	
Memphis, Tennessee	●	
Morehead City, North Carolina		●
Mount Vernon, Indiana	●	
Nawiliwili, Hawaii		●
NY/NJ Port Authority		●
Olympia, Washington		●
Panama City, Florida		●
Pascagoula, Mississippi	●	
Port Angeles, Washington		●
Port Canaveral, Florida		●
Port Everglades, Florida		●
Port Manatee, Florida		●
Port Newark-Elizabeth Marine Terminal, New Jersey		●
Port of Albany-Rensselaer, New York	●	
Port of Anchorage, Alaska		●
Port of Avery Lane, New Hampshire	●	
Port of Baton Rouge, Louisiana	●	
Port of Beaumont, Texas	●	

(continued on next page)

Table G-1. (Continued).

Port of Boston, Massachusetts		●
Port of Brownsville, Texas	●	
Port of Bucksport	●	
Port of Chicago, Illinois	●	
Port of Cleveland, Ohio	●	
Port of Corpus Christi, Texas	●	
Port of Eastport Maine	●	
Port of Everett, Washington	●	
Port of Honolulu, Hawaii		●
Port of Houston, Texas	●	
Port of Humboldt Bay, California	●	
Port of Jacksonville, Florida		●
Port of Lake Charles, Louisiana		●
Port of Los Angeles, California	●	
Port of Mack Point (Searsport), Maine	●	
Port of Miami-Dade, Florida		●
Port of Mobile, Alabama		●
Port of New Bedford, MA	●	
Port of New Orleans, Louisiana		●
Port of Oakland, California		●
Port of Oceanside, New Brunswick, Canada	●	
Port of Palm Beach, Florida		●
Port of Philadelphia, Pennsylvania	●	
Port of Port Lavaca - Point Comfort, Texas	●	
Port of Portland, Maine		●
Port of Portland, Oregon		●
Port of Providence, Rhode Island	●	
Port of Quincy, Illinois	●	
Port of Richmond, California	●	
Port of Richmond, Virginia	●	
Port of San Diego, California		●
Port of Savannah, Georgia		●
Port of Seattle, Washington	●	
Port of South Louisiana		●
Port of Stamford Harbor, Connecticut	●	
Port of Stockton, California		●
Port of Tacoma, Washington	●	
Port of Tampa, Florida		●
Port of Texas City, Texas		●
Portsmouth, New Hampshire		●
Valdez, Alaska	●	
Vancouver, Washington	●	
Wilmington, North Carolina		●

Abbreviations and acronyms used without definitions in TRB publications:

AAAE	American Association of Airport Executives
AASHO	American Association of State Highway Officials
AASHTO	American Association of State Highway and Transportation Officials
ACI–NA	Airports Council International–North America
ACRP	Airport Cooperative Research Program
ADA	Americans with Disabilities Act
APTA	American Public Transportation Association
ASCE	American Society of Civil Engineers
ASME	American Society of Mechanical Engineers
ASTM	American Society for Testing and Materials
ATA	Air Transport Association
ATA	American Trucking Associations
CTAA	Community Transportation Association of America
CTBSSP	Commercial Truck and Bus Safety Synthesis Program
DHS	Department of Homeland Security
DOE	Department of Energy
EPA	Environmental Protection Agency
FAA	Federal Aviation Administration
FHWA	Federal Highway Administration
FMCSA	Federal Motor Carrier Safety Administration
FRA	Federal Railroad Administration
FTA	Federal Transit Administration
HMCRP	Hazardous Materials Cooperative Research Program
IEEE	Institute of Electrical and Electronics Engineers
ISTEA	Intermodal Surface Transportation Efficiency Act of 1991
ITE	Institute of Transportation Engineers
NASA	National Aeronautics and Space Administration
NASAO	National Association of State Aviation Officials
NCFRP	National Cooperative Freight Research Program
NCHRP	National Cooperative Highway Research Program
NHTSA	National Highway Traffic Safety Administration
NTSB	National Transportation Safety Board
PHMSA	Pipeline and Hazardous Materials Safety Administration
RITA	Research and Innovative Technology Administration
SAE	Society of Automotive Engineers
SAFETEA-LU	Safe, Accountable, Flexible, Efficient Transportation Equity Act: A Legacy for Users (2005)
TCRP	Transit Cooperative Research Program
TEA-21	Transportation Equity Act for the 21st Century (1998)
TRB	Transportation Research Board
TSA	Transportation Security Administration
U.S.DOT	United States Department of Transportation