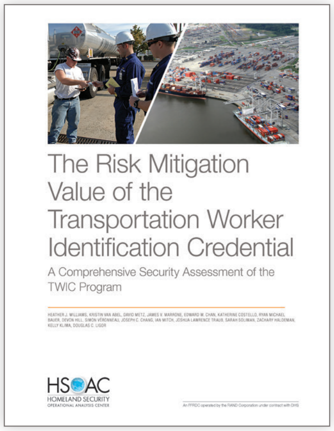
HSOAC HOMELAND SECURITY OPERATIONAL ANALYSIS CENTER
An FFRDC operated by the RAND Corporation under contract with DHS

RESEARCH SUMMARY


The Risk Mitigation Value of the Transportation Worker Identification Credential

A Comprehensive Security Assessment of the TWIC Program

HEATHER J. WILLIAMS, KRISTIN VAN ABEL, DAVID METZ, JAMES V. MARRONE, EDWARD W. CHAN, KATHERINE COSTELLO, RYAN MICHAEL BAUER, DEVON HILL, SIMON VÉRONNEAU, JOSEPH C. CHANG, IAN MITCH, JOSHUA LAWRENCE TRAUB, SARAH SOLIMAN, ZACHARY HALDEMAN, KELLY KLIMA, DOUGLAS C. LIGOR

HSOAC HOMELAND SECURITY OPERATIONAL ANALYSIS CENTER

An FFRDC operated by the RAND Corporation under contract with DHS

The Risk-Mitigation Value of the Transportation Worker Identification Credential: A Comprehensive Security Assessment of the TWIC Program

HEATHER J. WILLIAMS, KRISTIN VAN ABEL, DAVID METZ, JAMES V. MARRONE, EDWARD W. CHAN, KATHERINE COSTELLO, RYAN MICHAEL BAUER, DEVON HILL, SIMON VÉRONNEAU, JOSEPH C. CHANG, IAN MITCH, JOSHUA LAWRENCE TRAUB, SARAH SOLIMAN, ZACHARY HALDEMAN, KELLY KLIMA, DOUGLAS C. LIGOR

www.rand.org/t/RR3096

The Transportation Worker Identification Credential (TWIC) is designed to enhance security at U.S. ports. It demonstrates that the holder has passed a Transportation Security Administration security threat assessment and is required of anyone with unescorted access to a secure area at a regulated facility. This report provides the findings from an assessment of the TWIC program, along with the assessors' recommendations.

RESEARCH QUESTIONS

- Are the vetting standards appropriate for determining whether someone presents a security risk?
- Is the fee structure appropriate for the current costs of vetting?
- How long does it take for a Transportation Worker Identification Credential (TWIC) to be issued?
- Is TWIC unnecessarily duplicative of or redundant with other federal and state credentialing programs?
- Would requiring use of biometric readers at high-risk facilities yield a benefit greater than their cost?
- What alternatives exist to biometrics?
- What technology, business process, and operational impacts do TWIC and electronic readers have on facilities?

continued on back

KEY FINDINGS

The vetting standards might be appropriate, depending on stakeholder intent

- The security threat assessment (STA) would detect known or suspected terrorists who seek to legally gain persistent access to the maritime environment.
- The federal government and industry might have different objectives in determining risk, with the former focused on national security, the transportation sector, and terrorism and the latter also concerned about profits and worker safety.
- A single vetting standard must apply to the entire population working in the maritime sector, and facility management can adopt additional criteria beyond TWIC vetting standards to satisfy a facility's specific security needs.

Electronic biometric card readers would probably cost industry more than benefit it under the pending rule

- Readers are ultimately costly and mitigate only certain types of threats, forcing facilities to prioritize a source of vulnerability that might not be the most jeopardizing in their specific circumstances.

Electronic biometric card readers can mitigate some kinds of risk

- TWIC is stronger against attacks requiring persistent insider access than against those requiring one-time or no access.
- People more often gain unauthorized access to facilities via other means than by using invalid TWICs.

Further enhancing TWIC requirements would come at significant costs, which are likely to exceed the commensurate benefit

- There are likely more cost-effective methods of reducing the risk that maritime facilities face.
- There might be lower-cost options to bring greater security value from the TWIC program as currently implemented, such as a mobile application to allow facilities to check the Canceled Card List at essentially zero cost.

RECOMMENDATIONS

- Take a system approach to maritime security rather than focusing on one program. The effectiveness of a facility's security system overall matters far more than the effectiveness of any given component for any specific task.
- There is no one-size-fits-all solution for improving security at maritime facilities, given their broad differences in risk and operations. The current process of facility-specific security assessments and security plans is designed to enable flexible solutions specific to each facility's needs. Greater identity assurance methods might be appropriate for some facilities, given their risk profiles. Transparent management of the TWIC program with a focus on how to effectively support TWIC's stakeholders could incentivize industry to maximize TWIC's potential security benefit.

HSOAC is a federally funded research and development center (FFRDC) operated by the RAND Corporation under contract with the U.S. Department of Homeland Security (DHS). The HSOAC FFRDC provides the government with independent and objective analyses and advice in core areas important to the department in support of policy development, decisionmaking, alternative approaches, and new ideas on issues of significance. The HSOAC FFRDC also works with and supports other federal, state, local, tribal, and public- and private-sector organizations that make up the homeland security enterprise. RAND is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest. For more information, visit www.rand.org/hsrd/hsoac.