



**Testimony of Randall H. Walker
Director of Aviation, Clark County Department of Aviation
On behalf of Airports Council International—North America**

before the

**House Committee on Homeland Security
Subcommittee on Transportation Security**

“H.R. __, The MODERN Security Credentials Act”

May 4, 2011

Airports Council International-North America
1775 K Street, NW, Suite 500
Washington, DC 20006
(202) 293-8500

Chairman Rogers, Ranking Member Jackson Lee, and members of the Subcommittee, thank you for the invitation to appear before you today to offer the views of airport operators on the Modernizing of Documentation and Elimination of Redundant Identification and Security Credentials Act (MODERN Security Credentials Act). My name is Randall Walker and I am the Director of Aviation for the Clark County Department of Aviation which operates McCarran International Airport in Las Vegas, Nevada and four general aviation airports. I am testifying on behalf of the 344 member airports of Airports Council International – North America (ACI-NA) which enplane more than 95 percent of the domestic and virtually all the international airline passenger and cargo traffic in North America. More than 350 aviation-related businesses are also members of ACI-NA.

Before offering comments on the specific legislation, it is important to first understand the processes and procedures in place at airports to ensure applicants have been subjected to a background check prior to the airport issuing a Security Identification Display Area (SIDA) badge, which allows individuals to have unescorted access to secure areas of the airport.

SIDA Badge Process

Currently, applicants wishing to receive a SIDA badge must undergo a Security Threat Assessment (STA) to verify the individual's identity and allow the Transportation Security Administration (TSA) to utilize the Terrorist Screening Database and other government systems to ensure that the individual is a lawful resident of the United States and does not pose a security threat. TSA uses a variety of classified databases in order to perform the STA. Because of the sensitive nature of the results, TSA only provides airports with an approved status, indicating that the airport may grant the individual unescorted access to secured areas through the issuance of a SIDA badge, or a disapproved status, indicating that the airport must not issue the individual a SIDA badge or other form of identification. In addition, airports are required to submit an applicant's fingerprints to the FBI which conducts a Criminal History Record Check (CHRC). The results of the applicant's CHRC is sent to the airport so they can determine whether the individual has been found guilty (or not guilty by reason of insanity) of any of the 28 disqualifying crimes during the 10 years prior to the application for the SIDA badge. Some airports, through their TSA-approved airport security programs (ASPs), actually have a longer "look back" period or include additional disqualifying crimes; a process they believe enhances security at their airport and/or is required by state or local laws.

There is a process in place which allows individuals to seek redress if they have been denied a SIDA badge due to information received from a CHRC or STA. If the individual has been denied airport credentials based on the results of a CHRC, TSA regulations require that the airport operator advise the individual that the CHRC discloses information that would disqualify him or her from receiving or retaining a SIDA badge and provide the individual with a copy of the FBI record if the individual requests it. TSA regulations also allow corrective action by an individual if he or she believes the FBI records are inaccurate. Regulations state that the individual may contact the local jurisdiction responsible for the information and the FBI to complete or correct the information contained in his or her record within 30 days after being advised that the CHRC discloses a criminal offense. The individual must also notify the airport

in writing of his or her intent to correct any information they believe to be inaccurate. The airport operator must obtain a copy, or accept a copy from the individual of the revised FBI record or a certified true copy of the information from the appropriate court, prior to issuing the individual a SIDA badge granting unescorted access.

If through an STA, the TSA determines that an applicant does not meet the requirements and is denied an airport-issued badge, TSA will provide the individual:

- (i) A statement that TSA has determined that the applicant does not meet the eligibility requirements to hold an airport approved and/or airport issued personnel identification media;
- (ii) The basis for the determination;
- (iii) Information about how the applicant may appeal the determination; and
- (iv) A statement that if the applicant chooses not to appeal TSA's determination within 60 days of receipt of the Initial Determination, or does not request an extension of time within 60 days of the date of service of the Initial Determination of Threat Assessment in order to file an appeal, the Initial Determination will automatically become a Final Determination of Threat Assessment (FDTA) without further notification from TSA.

TSA, not the airport authority, makes a determination as to whether an applicant's STA reveals information that the individual does or does not pose a security threat. Redress based on the STA will be handled on a case-by-case basis due to the classified and/or security sensitive information that may be involved. TSA is the final adjudicator of STA results.

In addition to the STA and CHRC, TSA regulations require individuals seeking a SIDA badge to complete training provided by the airport.

Pursuant to regulatory guidance issued in 2002 and subsequent Security Directives, TSA requires all airports and airlines to use and pay the Transportation Security Clearinghouse (TSC) for its email messaging services to consolidate and transmit the biographic and biometric data necessary for TSA to conduct Security Threat Assessments (STAs) and the FBI to conduct fingerprint-based criminal history record checks (CHRCs). In accordance with the requirements, airports collect the required biographic information of applicants for airport-issued identification badges, input the data in a spreadsheet and transmit it to the TSC. Similarly, airports collect the fingerprints of SIDA badge applicants and transmit them electronically to the TSC. The TSC simply consolidates the information and transmits it to the TSA.

The TSC is not uniquely qualified to perform this function. Indeed, at least eighteen companies, in addition to the TSC, have been certified by the FBI as being qualified to transmit data pursuant to federal standards. With the expansion of background check requirements by state and local governments and the commercial sector, the FBI has developed a testing process for certifying companies that meet federal standards to perform the function.

Almost three years ago, as Chairman of ACI-NA, I sent a letter urging TSA to provide a fair, open competitive process by allowing airports – and other industry stakeholders – to utilize other channeling service providers. Around that time, several other airports sent letters with similar requests to TSA. To date, TSA has not allowed airports to choose between qualified vendors

providing such services. My concern is not specifically with the TSC providing channeling services. Rather, it is that TSA has precluded fair and open competition in the marketplace in not allowing airport operators a choice between FBI-certified vendors that provide channeling services.

SIDA vs. TWIC

The SIDA background check process and that for the Transportation Worker Identification Credential (TWIC) are distinctly different and affect very diverse workforces between the transportation modes, all of which may be faced with dissimilar threats. In the case of the SIDA badging process, the airport (the employer in most cases) grants unescorted access to certain areas of their individual facility. The ability for airport operators to monitor and limit individuals' access to certain areas at an airport is an essential layer of security that would be compromised under TWIC, which would allow a badge holder to access virtually any area of an airport. At a minimum, airports comply with strict regulations for STAs and CHRCs but again, some airports, because of state and local laws, go above and beyond the federal minimums with regard to disqualifying offenses. Airports must follow TSA regulations, but unlike TWIC, identification badges are issued by the airport, not the federal government. It is also important to note that just because an individual has held or currently holds a SIDA badge from one airport it does NOT grant them unescorted access to secure areas of another airport. Due to the need for airports to limit individuals' unescorted access to certain locations within the secured area and given the vast differences between commercial aviation and port facilities, airports do not believe it makes sense to align the SIDA and TWIC processes.

MODERN Security Credentials Act

Although they are both agencies under the Department of Homeland Security (DHS), current TSA and Customs and Border Protection (CBP) regulations require separate and duplicative biometric and biographic data submissions to support background checks for aviation employees that are subject to the requirements of each agency. Rather than requiring separate data submissions to satisfy various agencies such as TSA and CBP, airports believe DHS should develop a consolidated system for background check data submissions for aviation workers. Airports support Congress helping to move TSA and DHS toward that goal.

With regard to the MODERN Security Credentials Act, airports appreciate and support the language that reiterates the airport operator's right to restrict an individual's access to secure areas. Additionally, airport operators support the language which preserves their right to disqualify an individual from employment based on their review or adjudication of a criminal history record check. Although the legislation does contain some protections, airports have identified some concerns with the bill.

First, the rulemaking language is overly broad and unnecessary for TSA to move forward with its rulemaking to align the requirements and fees for background checks, something that is already underway. While this language appears to only affect the STA process, proposed changes to section in the U.S. code in the legislation actually affect the process for CHRCs. This could mean that the STA and CHRC processes would be merged under this rulemaking and that airports would no longer be able to review or adjudicate CHRC results. Merging these processes could be problematic, as not all airport credentials give unescorted access to the secure area.

Current TSA background check requirements stipulate that certain individuals should only be subject to an STA. If these processes are merged, it could mean that additional individuals – who have no need for unescorted access to secured airport areas – would be required to get a CHRC, simply because they operate near or in an unsecured area of an airport. This could impose significant operational issues and unnecessarily drain limited resources while significantly increasing costs. For example, construction personnel working on airport projects do not have unescorted access and therefore, are only required to have an STA. Airports have existing effective measures in place to ensure that these personnel do not go into the SIDA area. Expanding the current requirement to include this population is unnecessary and could cause significant delays in these projects while workers wait for the processing of their CHRCs.

Airport operators agree that DHS should be required to consult with various stakeholders, including airports as they develop the rule. However, the consultation language provided in the bill does not require recommendations by stakeholders to be considered as part of or inform the rulemaking process, which allows the agency to disregard any comments made by stakeholders during the consultation process.

Furthermore, the limitation language in the bill protects the current process at airports with regard to the background checks. But, if this legislation is enacted before TSA has changed the security directive and regulatory guidance which requires airports to use the TSC, this could be interpreted by TSA as a ban on competition for channeling service providers, thus protecting the TSC's sole-source contract and the requirement that airports use only TSC as their channeling service provider. ACI-NA has long advocated for TSA to allow airports a choice between qualified vendors, including the TSC, that consolidate and transmit the required biographic and biometric information for STAs and CHRCs. ACI-NA asks that the language be modified to protect competition among channeling service providers.

Airports support the requirement in the bill that the agency provide an analysis of how the STA process will be consolidated; any reductions in fees or costs; and any other efficiencies that the rule may realize. However, the new process put forth by the rule could cause operational delays in getting responses back from TSA about whether individuals are cleared. ACI-NA believes TSA should also be required to conduct a thorough examination of the potential operational impacts resulting from the requirements prior to issuing a notice of proposed rulemaking.

Although the bill contains specific language preserving the current process for airports to determine whether to issue individuals a SIDA badge granting unescorted access to secured areas, it also contains contradictory or conflicting language requiring the Secretary to determine whether an individual is qualified to receive a badge based on the results of the CHRC. This language would prevent airports from adjudicating results of a CHRC or imposing more stringent security requirements that are necessary for the unique security challenges at their airports. Airports strongly oppose this language and believe that the results of the CHRC should be adjudicated at a local level. Again, some airport operators, to enhance security in accordance with their TSA-approved airport security programs or because of state and local laws, choose to include additional disqualifying crimes or a longer "look back" period than is required by federal law. Airports reiterate that it should remain a local decision to implement more stringent security requirements.

Because there is a process in place which allows individuals to seek redress if they have been denied a SIDA badge based on the results of the CHRC, airports believe there is no need for individuals denied unescorted access to secured areas to participate in the TWIC waiver process. While airports appreciate the language in the bill which protects the rights of airports to disqualify any individual from employment based on a review or adjudication of a CHRC even if the individual hold a waiver, there is concern about the potential for implied pressure some airports might receive from TSA over granting unescorted access to individuals that have received a waiver, particularly for TSA's own employees as has occurred previously. Airports also support the language which protects them from being sued for refusing to provide unescorted access to individuals that have been determined to have some derogatory information as part of their background check.

As a result of the rulemaking required in the bill, airports will be faced with a significant increase in fees for STAs, a cost which TSA currently covers. Additionally, the legislation allows the costs of the waiver process to be incorporated into the fee. With a process already in place for individuals to correct inaccuracies identified in their CHRC and STA results, airports do not believe there is a need for a separate waiver process. ACI-NA is concerned that incorporating the costs of a waiver process and imposing a new fee for STAs will significantly increase costs. Again, while this may allow the fee for other populations within the transportation sector to be lowered, it will significantly increase fees in the aviation sector. Airport operators do not believe they should be forced to pay for the costs of a formal waiver process within TSA.

Conclusion

Although ACI-NA supports the goal of developing a consolidated system for the submission of data to support background checks for aviation workers, this bill includes conflicting requirements that would cause unintended and unnecessary operational challenges, and impose additional costs for airports. In order to ensure that the requirements are operationally feasible and commercially competitive, airports encourage the Committee to direct TSA to constitute a government and industry working group, tasked with making recommendations for streamlining the current process, which would be incorporated into a notice of proposed rulemaking.

Airports believe very strongly in and are determined to retain their right to deny individual's unescorted access to secure areas at their airport. If an airport operator chooses (whether because of state and local laws or in order to enhance security) to include additional disqualifying crimes or a longer "look back" period than is required by TSA, it should be their prerogative to implement more stringent security requirements.

While airports continue to urge DHS to develop a consolidated system for background check data submissions for aviation workers as a way to reduce costs and streamline the process, airports oppose the implementation of a credential which would provide universal access for aviation workers or for aviation workers to be absorbed into TWIC.

ACI-NA looks forward to working with the Committee, DHS and TSA to identify procedures to increase the effectiveness and efficiency of the background check process for aviation workers while preserving the ability for airports to adjudicate results, make decisions about whether to grant unescorted access privileges to individuals and to determine the level of access based on job function.

Thank you for the opportunity to appear before you today.