DEPARTMENT OF STATE

STATEMENT
OF
BRENDA S. SPRAGUE
DEPUTY ASSISTANT SECRETARY FOR PASSPORT SERVICES

BEFORE THE
HOUSE COMMITTEE ON HOMELAND SECURITY
SUBCOMMITTEE ON BORDER AND MARITIME SECURITY

HEARING
ON
PASSPORT FRAUD: AN INTERNATIONAL VULNERABILITY

FRIDAY APRIL 4, 2014

Chairman Miller, Ranking Member Jackson Lee, thank you for the opportunity to testify today about the many things the Department of State does to promote security through interagency cooperation, international data sharing, and integrity of the U.S. passport.

First, I'd like to offer my thoughts and prayers to the family and loved ones of those on Malaysia Airlines Flight 370. Our heartfelt thanks go out to the international effort of men and women working around-the-clock to solve the mystery of this plane's disappearance.

The initial investigation uncovered a troubling case of imposters using stolen Austrian and Italian passports to board the Malaysian jetliner. Although it might not be related to the plane's ultimate fate, this episode underscores the importance of continued and comprehensive data-sharing among the federal and international communities to prevent acts of international terrorism, illegal immigration, and other serious forms of international crime, as well as theft or misuse of passports.

The State Department works closely with our colleagues at the Department of Homeland Security, the Department of Justice, and other agencies to ensure our documents, and reports of their misappropriation, are shared broadly and quickly.

Domestically, we do this through data-sharing of U.S. lost, stolen, and revoked passport data to TECS, a system used by the U.S. Customs and Border Protection to screen arriving travelers at ports of entry. We also send to TECS information we receive about lost and stolen foreign passports.

Internationally, we have been in the forefront of a significant push to promote reporting of lost and stolen passport data to the INTERPOL Stolen and Lost Travel Document—or SLTD—database. The State Department provides INTERPOL with comprehensive, real-time data on lost, stolen, and revoked U.S. passports—including the passport number and date of issue—so it is accessible to member law enforcement authorities worldwide. Annually, about 300,000 U.S. passport books and 20,000 passport cards are reported by U.S. citizens as lost or stolen – resulting in more than 3.2 million reports to the SLTD database since we began participating in 2004. The Department chose to add revoked passport data to the SLTD in 2010, and since then, have reported more than 3,500 revoked passports.

The Departments of State and Homeland Security use SLTD to vet visa applicants, inbound flight and vessel manifests, and land border crossers at U.S. ports of entry. U.S. Customs and Border Protections officers at U.S. ports of entry send to the Department seized U.S. passports which we analyze to look for patterns and determine whether the bearer submitted a fraudulent passport application. Applications that exhibit evidence of fraud, complicity in alien smuggling, or other derogatory information are then referred to Fraud Prevention Managers in the domestic passport agencies and centers, and Diplomatic Security field offices for further investigation and possible prosecution. Where warranted, this information might be input into internal systems to be used if the bearer of the passport applies for another passport.

On the international front, the State Department works with member countries of the Asia-Pacific Economic Cooperation (APEC) alliance to detect documents reported as lost or stolen. This program, called the Regional Movement Alert System—or RMAS—is geared toward preventing criminals from boarding flights to participating countries. We are also engaging Taiwan—a non-INTERPOL member—to provide direct two-way transmission of lost, stolen, and revoked U.S. and Taiwanese passport data.

Perhaps most importantly, U.S. law requires all 37 countries participating in the Visa Waiver Program (VWP), as well as Taiwan, to report lost and stolen passport data to the United States Government via INTERPOL or through other means designated by the Secretary of Homeland Security. We believe approximately 70 percent of the SLTD's current data comes from VWP countries. The Department of State cannot compel foreign countries to check against this database; however, the Department does automatically screen against the SLTD database – i.e., electronic applications of immigrant and nonimmigrant visa applicants are screened against the INTERPOL database to ensure they are not using a passport that was reported lost or stolen.

Despite the Department's important domestic and international efforts to track reports of lost, stolen, or revoked documents, challenges remain which must be addressed. That's why the State Department must have other fraud prevention tools to help us verify citizens' identity and entitlement to a U.S. passport.

The U.S. passport is one of the most sought-after documents in the world. Although primarily used for international travel, it is also a legal form of

identification and might be used to verify eligibility for Social Security, healthcare, or entitlement benefits. It can also be used to apply for a driver's license, obtain a mortgage, and verify employment eligibility. A passport is also one of the few photo identification documents available to minors and can be used in support of school enrollment or educational assistance. These key points, along with the message of keeping the passport secure, are communicated to the public at outreach events, through the travel.state.gov website, and through social media tools.

Because of the access a passport provides, we have invested in high-tech security features including photo biometrics, secure laminates, micro-printing, color shifting security ink, and enhanced electronics that render these documents virtually impossible to counterfeit.

As the sophistication and complexity of the U.S. passport has increased, so have the efforts of those attempting to commit passport fraud. The days of carefully peeling back the cover to replace the photo in a U.S. passport are long past. Today's passport fraud most often involves fraudulent supporting identity ("breeder") documents: fraudulent birth certificates, false identities, and look-alike

photos (sometimes with the cooperation of the legitimate bearer), are a few of the methods employed by imposters and other criminals.

To counter breeder document and identity fraud, we employ a robust fraud prevention strategy that includes in-depth training to our adjudicators, verifying information against government and commercial databases, and technology, such as facial recognition. Our employees receive twice-monthly training to identify various types of fraud and highlight current trends in this type of fraud. We also integrate several real-time, front-end database checks into our adjudication system including facial recognition, Social Security, and death record verifications.

During the adjudication process, we use the National Law Enforcement Telecommunications System network to verify drivers' licenses. We run checks against files from the FBI to identify people on probation, parole, or pre-trial release who might be trying to obtain a U.S. passport to flee the country. Additionally, we use the services of several commercial data providers which allow our employees to verify an applicant's social footprint and detect fraudulent addresses, phone numbers, and other discrepancies in their application information.

Though I believe our systems and processes are strong, none is ever invulnerable. That's why we continually review our methods to improve issuance and fraud detection and look for new ways to strengthen existing procedures.

In this vein, we are currently developing a system that will allow citizens to report lost and stolen passport books and passport cards online immediately, thereby speeding the information-sharing process. We chair an interagency working group that meets weekly developing a next generation passport product that might include—among other advanced features—laser-perforated pages to prevent page substitutions.

The Department engages actively with state vital records bureaus to encourage contributions to a national centralized database of birth and death records provided by The National Association for Public Health Statistics and Information Systems. We are implementing a Memorandum of Understanding with the Federal Bureau of Prisons, and engaging state corrections agencies to share parole and pre-trial data.

To protect our citizens and promote safe, secure and legal travel throughout the world, we welcome opportunities to continue to expand these efforts with federal, state, local and international agencies.

Thank you again for the opportunity to appear before you today. I am happy to answer any questions you might have.