WRITTEN STATEMENT OF

KATHLEEN CARROLL

BEFORE THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

UNITED STATES HOUSE OF REPRESENTATIVES

SECURE IMMIGRATION IDENTITY DOCUMENTS

PRESENTED OCTOBER 21, 2015

Statement of Kathleen M. Carroll
Vice President of Corporate Affairs
HID Global, Inc.
House Committee on Oversight & Government Reform
October 21, 2015

Good morning Chairman Chaffetz, Ranking Member Cummings and other distinguished members of the Committee. Thank you for inviting me to testify today.

My name is Kathleen Carroll. I am the Vice President of Corporate Affairs at HID Global, Inc. where I focus on the intersection of technology, security and policy, with a particular focus on privacy. I am honored to be able to share with you HID Global's concerns regarding the manufacture and procurement of secure immigration identity documents.

HID Global is the world's leading manufacturer of secure identity credentials, including the US Green Card. We are headquartered in Austin, TX and employ highly skilled workers in high-paying manufacturing jobs in our Austin facility. That facility has been certified by the Department of Homeland Security as being a secure facility for the manufacture of secure credentials for the US Government. For more than 25 years, we have been designing, developing and manufacturing secure credentials and/or their component parts for private businesses and governments around the world, including passports for more than 25 countries, government-issued ID cards, and, as I mentioned, the US Green Card. In fact, HID makes your Congressional staff ID cards and Member voting cards.

HID Global is part of a robust private industry of competitors and customers that together have continued to innovate and improve the functionality and security of these secure credentials over the decades since the technology was invented. HID Global and our competitors are constantly evolving technologies and strategies to thwart counterfeiters and those that would do us harm.

For years, we have invested in and mastered the complex manufacturing process to make the secure credential components work seamlessly and flawlessly. The security of our nation depends on these systems as our first line of defense at the borders.

A simple, easy to replicate card can certainly be made by untrained people with readily available equipment. A complex, hard to replicate, easy to use, reliable card is actually very difficult to make and requires specialized expertise and training. But the card is only part of the solution. There is an entire infrastructure The design can include digital storage, antenna to communicate the data to a reader or scanner, and software to make all of that electronic transmission and translation work seamlessly and consistently. Congress needs to decide which they want to have for the identity documents relied on at our borders.

This is why companies like HID Global exist – because we have mastered the development and execution of not only making the card, but of designing and building the entire system. We also design and sell the components of those systems to some of our competitors – but it is the knowledge and expertise in the end-to-end solutions, and the ability to make them all communicate with each other securely, that makes it all work. That is why the HID-made US Green Card has consistently been considered the hardest to counterfeit government-issued ID card for so many years, and why we have a read-rate of around 98% - meaning the border agents and other law enforcement officials can have confidence that when they scan the card, they will be able to quickly and accurately determine the legitimacy of the card holder.

However, we are not satisfied with that success. We spend millions of dollars every year, and hire the best experts, to continually upgrade the security and the effectiveness of our technology. New manufacturing processes, new designs, new materials, new techniques. We know that the bad guys are trying to replicate our technology and create fake documents to fool border agents and law enforcement and gain unlawful entry into the United States. Congress created these programs and mandated these card programs for a reason – to secure the border. We are proud of the jobs we create and the technology we develop to help you do that; and we hope to continue doing so in the future.

Our ability to do so, however, is threatened by the decision by the Government Publishing Office (GPO) to become a manufacturer of secure credentials as a government agency. With no legislative direction or authority from Congress, the GPO has broadly interpreted its mandate under Title 44 – which created the GPO to provide printing services for the Legislative Branch – to become a manufacturer of secure credential technology. The GPO is also aggressively marketing its manufacturing services to Executive Branch agencies with a legal claim that it is the sole legal source of these secure credentials, because Title 44 made them "the Government's printer."

Under this extreme interpretation of the definition of "printing," there is nothing to prevent the GPO from declaring tomorrow that email is a form of digital "printing" and become a manufacturer of laptop computers, or .pdf documents are a form of digital publishing, and develop software to compete with Adobe or Microsoft. Except the GPO doesn't really intend to compete at all. They instead inform the Executive Branch agencies that they are required to obtain secure credentials from the GPO under Title 44. We would love to be able to tell our customers that they are required by law to buy their products from HID.

The GPO began asserting this in 2007. We were part of a team of private industry vendors who spent months developing cutting edge secure identity documents for the Consolidated Trusted Traveler RFID Card Program.

Late in the procurement process, we were abruptly informed by letter that the GPO would provide the cards. The letter cited a technically irrelevant requirement and Title 44.

Instead, HID has consistently earned the US Green Card business by delivering a secure immigration document that has an extremely high electronic read rate, and an unparalleled track record of being counterfeit resistant. Among the security features we innovated and integrated into the Green Card design is a technology known as an optical stripe – a metallic stripe embedded into the laminate that is laser-engraved with a high-resolution replica of the card-holder's face and signature. It is easy to visually confirm its authenticity; it holds digital data that must be programmed to match the data printed on the card; and is virtually impossible to replicate without very sophisticated and hard-to-obtain laser engraving technology.

The GPO does not have the capability to utilize technology like the optical-stripe; yet it is not technology that is proprietary to HID. Even if it were proprietary, it seems the threshold question Congress should be asking is "how do we make our government-issued credentials, used to enter the United States, as secure as possible?" Not: "How do we ensure that the GPO or any other entity that wants to enter the market to manufacture credentials can do so?"

We recently were re-awarded the contract to manufacture the US Green Card under a competitive bidding process with other private manufacturers. We intend to work with USCIS to continue making the most secure, most reliable credential on the planet. That competition almost didn't happen. We learned that the GPO had been having conversations with the USCIS for months prior to the release of the most recent Request for Purchase (RFP) for the US Green Card. The GPO was asserting that USCIS could avoid the complicated and rigorous process of conducting a competitive bid from private sector vendors and instead simply request the Green Card be awarded to GPO under Title 44.

We also learned that the GPO was urging USCIS to drop or modify some of the security features that have worked so well in the Green Card to thwart counterfeiters – like the optical stripe – so that the card requirements were something the GPO had the technical capability to design and manufacture. Fortunately for our national security, the USCIS ultimately rejected the GPO's suggestions to "dumb down" the Green Card so GPO could manufacture it.

Congress has created a number of programs focused on the issuance of secure credentials to verify a person's identity and confirm their right to be in the United States. Green Cards, Passports, border crossing cards, etc – were all intended to be the first line of defense for the United States to accurately determine who is allowed to be in the country or not.

Congress needs to decide if your goal is to have the best, most secure, most advanced secure credential technology to protect the border. If so, you need to enforce the policy that agencies should buy the best and most secure credentials from those of us in industry that have invested our innovation and expertise to invent the best. If the goal is to be a government jobs program, or to provide a revenue stream to help the GPO cover their fixed costs to maintain an obsolete printing infrastructure, then Congress should clearly and legislatively authorize the GPO to create this business unit.

To argue that the manufacture of secure credentials is somehow a uniquely governmental function is to ignore the history of how secure credentials were invented and created in the first place by the private sector. By that reasoning, building laptops and desktops for government employees is a uniquely governmental function. Building phones for government employees is a uniquely governmental function. Developing and manufacturing drugs for VA patients is a uniquely governmental function. Developing and writing software to secure government networks is a uniquely governmental function.

Congress needs to decide where to draw that line, not the GPO itself. By its own admission, and its own published business plan, the GPO is counting on the revenue stream from the manufacture and sale of secure credentials. The government agencies are paying GPO with appropriated dollars at taxpayer expense. The GPO should not be the sole decision maker on whether they are meeting or exceeding their mandate.

Kathleen M. Carroll

Kathleen Carroll is Vice President, Corporate Affairs for HID Global, a worldwide leader in secure identity solutions. Carroll serves as an ambassador, spokesperson and representative for HID Global. She oversees the company's privacy and policy initiatives to support its brands around the world. She also works to support public policies that address cybersecurity and privacy at the national and international levels.

As part of her responsibilities, Carroll chairs the Security Industry Association's (SIA) Government Relations Committee which works to educate legislators, business leaders and consumers about security technologies and their benefits across a spectrum of applications, including identity management, physical and logical (cyber-security) access control, food and drug safety, child safety, and patient safety. Carroll also sits on the National Security Task Force at the U.S. Chamber of Commerce.

An Advisory Board member for the Identity Center at the University of Texas at Austin she is a frequent speaker at industry events, discussing the intersection of privacy and technology and the implications for both the public and private sector as this issue rapidly evolves. In addition, she chairs the Privacy and Public Policy working group within the International Biometrics and Identification Association (IBIA). Carroll also serves on the Advisory Board for Mission 500, a non-profit organization dedicated to serving the needs of children and communities in crisis.

A magna cum laude graduate of Temple University, Carroll earned a BA in Journalism. She is a member of the International Association of Privacy Professionals and a Certified Information Privacy Professional and a Certified Information Privacy Professional/Government.