Remarks of Duane Blackburn
Assistant Director, Identity Management and Homeland Security
Office of Science and Technology Policy
Executive Office of the President

at the

Biometric Consortium Conference
September 27, 2011

"We have some planes."

Try to imagine the thoughts of the Boston Air Traffic Controller upon hearing this transmission on the morning of September 11, 2001:

- "Who is that?"
- "Who should I share this information with?"
- "What else do we know that should be linked with this information?"

-- Questions asked by a solitary Federal official in the fog of a war that he didn't yet know was taking place.
-- Questions asked by Federal identity professionals in the fog of technology, policies, and bureaucracy every day since.

9/11 was a day that had started with remarkable clarity and calmness, but quickly devolved to confusion and nervousness as citizens throughout the Nation watched the response and recovery activities at the World Trade Center and the Pentagon. Citizens then took action, forcing the terrorists on the fourth hijacked airliner to abandon their plans to attack yet another national symbol. Just as it took some time for Flight 93 passengers to learn what was taking place and to decide how to take action, the U.S. Government also took some time before it initiated military action overseas while simultaneously implementing numerous new security capabilities at home. Biometrics was to play a key role in both theaters because of the criticality of identification in operational activities – a tool that had been exploited by the terrorists themselves, as all but one of the 19 obtained and used U.S. identification documents.

This is the eighth and final time that I have the privilege of participating in a Biometric Consortium Conference in my role of coordinating Federal biometric activities out of the White House's Office of Science and Technology Policy. The amount of progress that this community has made over this period is truly astonishing, and the impact that you have had in securing our country has been considerable. Our progress and impact has been enabled through collaboration – collaboration within the Federal government, collaboration across the private

sector, and numerous public-private partnerships. Our activities, and the manner in which we pursued them, has been followed, supported, and praised by two separate presidential administrations. Each group of individuals within this community deserves praise:

- Biometric Consortium. The Consortium was a bit unstable on 9/11 as the policy-level oversight entity that it reported to had been recently terminated. It stabilized and evolved into what you see today: the preeminent worldwide gathering place to discuss biometrics. Jeff, Fernando, and Dick deserve a thank you from each of us for their commitment to this conference.
- Educational Professionals. In the days following 9/11, we quickly realized that individuals with adequate educational background and practical biometrics experience were in short supply. Today we have biometrics and identity management courses, degrees and professional certifications that provide the training necessary for our community to function.
- Researchers and standards organizations. Your advancements have been absolutely stunning! The core capabilities of today's technologies are orders of magnitude better than they were on 9/11. The availability and use of standards, long an indicator of a technology's maturity, has enabled our system of identity systems to function.
- Biometric companies. After a rough start, biometric providers responded to provide vastly improved products that continually perform as we expect and need them to. You are the backbone of our current capabilities, and our future success depends on your stability and ingenuity.
- System Integrators. Biometric technologies are but one piece of a functioning operational system. Fortunately, there are dozens of competent system integrators with experience developing complex systems for federal government and private sector applications that have done a wonderful job of incorporating biometric technologies.
- Privacy professionals. There wasn't a single departmental privacy official on 9/11, but the first one brought aboard immediately dove into identity issues. Many of the lessons learned in our initial work were applied to other technology issues as well, making this young field of biometrics a graybeard in the application of privacy theory within the federal government. We now have a cadre of privacy and civil liberties professionals throughout the federal government that are successfully integrating their principles throughout a biometric system's lifecycle.
- Intel Analysts. The newest entrant into the biometrics community is intelligence analysts. While it may be difficult enough to recognize someone with a biometric system, it is even more difficult to figure out what to do about the hit. It is this "so what" question that intel analysts answer. They have quickly gained knowledge on biometric systems, and what the hits mean, and seamlessly incorporated this new bit of information into their analyses. Working out of sight, and usually unknown to the world, these are the individuals who transform our technical capabilities into operational successes.
- Finally, Federal program managers and policy officials. This is the group that I have worked the closest with over the past eight years, and they have inspired me every day. It is impossible to comprehend how difficult it is to collaborate across stovepipes inside

the federal government without living in it firsthand. Oversight structures, the budget process, and even personnel evaluations seemingly conspire to convince them that collaboration is too risky or just plain not worth their time. Federal officials leading biometric activities have consistently overcome these hurdles and redoubled their efforts to collaborate with, and provide free assistance to, their partners throughout the federal service. I have worked on and led collaborative endeavors on a variety of other topics within the White House, but none of them have embraced the necessity and benefits of working together as much as your Federal biometrics leadership has. This has often been a thankless task for them, until now. Thank you all.

While we celebrate the progress and impact enabled by the biometrics community throughout this week, we cannot relax and sit back contently. Threats to our homeland and national security remain, and our adversaries are constantly studying our defensive postures -- they are certainly looking for holes in our layers of identity protections. Because of this, we must also move forward and continue to advance this technology so that we can provide even better operational capabilities in the future. To that end, the NSTC Subcommittee on Biometrics and Identity Management is releasing a 2011 update to *The National Biometrics Challenge.* This new report provides an overview of current challenges related to strengthening the scientific foundation of biometrics and improving identity management system capabilities. It clarifies biometrics-related priorities for Federal agencies and provides context for non-governmental entities considering collaborations with agencies as private-sector partners.

This community rose to the challenge issued in 2006, and I ask that you do so again today. Use this conference to learn what we are currently capable of, to discover groundbreaking opportunities for improvement, to foster collaboration, and to re-enlist in *your* community for the next ten years.