

**Todd M. Keil**

**Opening Statement before the House of Representatives, Committee on  
Oversight and Government Reform**

**Washington, DC**

**September 30, 2014**

Thank you, Chairman Issa, Ranking Member Cummings and distinguished Members of the Committee for inviting me to testify today regarding the U.S. Secret Service's security protocols in light of the September 19, 2014, incident in which an armed intruder entered the North Portico of the White House.

I believe I can offer a unique perspective on the management, procedural, physical and technical aspects of protecting high-visibility, targeted facilities after spending a career of almost 23 years as a Special Agent with the U.S. Department of State's Diplomatic Security Service with responsibility for developing and implementing security programs for U.S. personnel and embassies, consulates and other official facilities around the world. I have also spent numerous years in the private sector working in and advising corporate security operations and management. Additionally, from late 2009 until early 2012, I was the Assistant Secretary for Infrastructure Protection at the Department of Homeland Security. As the Assistant Secretary, I was responsible for public-private partnerships and a regulatory program to protect the critical assets of the United States essential to our nation's security, public health and safety, economic vitality and way of life. Last year, I also was selected and served on the Benghazi Accountability Review Board recommended Independent Panel on Best Practices which was established to identify best practices from across U.S. government agencies, the private sector, non-governmental organizations and allied countries on management and operations in high-threat, high-risk locations globally.

Mr. Chairman, the United States Secret Service has a proud history of almost 150 years protecting the most important government leaders of our country, the White House and other official facilities and conducting criminal investigations to ensure the integrity of our currency, banking systems and financial communications and cyber security. The men and women of the Secret Service are on the front line everyday keeping our nation safe and they do a tremendous job. The agents and officers of the Secret Service are constantly in the spotlight, serving at the White House, one of the most prominent symbols of our nation's strength and democracy, and we owe them a debt of gratitude for their service to our country.

Every organization, however, and even those with a century and a half of history, must be willing to learn.

Those who wish to do us harm, from a unpredictable, lone, possibly mentally unstable person, to an organized terror group intent on unleashing a calculated attack, typically have the element of surprise. Our country today faces a very dynamic, fluid and evolving threat environment in which the aggressors have become very patient, resilient and determined. We have to be better than they are! To counter this threat, security and law enforcement agencies, like the Secret Service, must have solid strategic and tactical management and leadership, focus on their primary mission, provide their people with the best training and resources and, possibly most important, be nimble and flexible. The Secret Service, like any successful organization, must be willing to continuously evolve and improve to adapt the agency ahead of the threat curve.

Throughout my career, I have found that government agencies and private sector organizations, who are at the top of their game, become complacent. Time tends to unknowingly erode and blunt the pointy end of the spear, and organizations and their management teams rely on, "this is the way we have always done it" or "we know how to do this best," so they are unwilling or unable to change. The Secret Service, I believe, would benefit from expanded use of new and emerging technologies to assist with its protective security responsibilities. In fact, when I was at the Department of Homeland Security, the Secret Service partnered with my office and the DHS Office of Science and Technology to research and develop cutting-edge technology for use at major events in the United States. Now is the time to bring some of those technological enhancements out of the lab and expand their use in the Secret Service toolkit. In addition to emerging technology, management and leadership of an organization must adapt, change and improve. Policies, procedures, and deployment of personnel and resources should be under constant scrutiny and exercised based on real world scenarios. The officers and agents of the Secret Service are some of the best this country has to offer and they deserve the strategic and tactical leadership to match.

All too often, Mr. Chairman, after something has gone wrong, the cry is simply for more money and more bodies. This is rarely the correct answer. Absent a comprehensive understanding of the foundational issues that led to systematic failures, throwing more money and people at the problem will only exacerbate existing management weaknesses and compound and magnify rather than correct management challenges.

Internal reviews post incident are typical in the U.S. government, from agency to agency, but, from experience, those reviews are impacted by intentional or unintentional personal and professional bias and often are informed by the same agency cultural and management weaknesses that may have been a contributing factor in the original incident. The Department of Homeland Security (DHS) and the Secret Service now have a unique opportunity and critical moment in time to obtain an unbiased, independent top to bottom review focusing on the Service's management, and policies and procedures related to the incident on September 19<sup>th</sup> and other similar incidents involving unauthorized persons entering the White House complex. I recommend that the Secretary of Homeland Security appoint a panel of external, independent experts to conduct this review and this group should be tasked with providing advice, guidance and formal recommendations to DHS and the Secret Service.

Mr. Chairman, throughout my career I have always been proud to work side by side with my Secret Service colleagues at every level in the agency. The United States Secret Service is a recognized world-class organization, and I am confident they will learn from this most recent and related incidents and innovate, strengthen and improve as they keep our country and our leaders safe.

Thank you, Mr. Chairman and Committee members, and I am happy to answer any questions you may have.

Committee on Oversight and Government Reform  
Witness Disclosure Requirement – "Truth in Testimony"  
Required by House Rule XI, Clause 2(g)(5)

Name:

1. Please list any federal grants or contracts (including subgrants or subcontracts) you have received since October 1, 2011. Include the source and amount of each grant or contract.

NONE

2. Please list any entity you are testifying on behalf of and briefly describe your relationship with these entities.

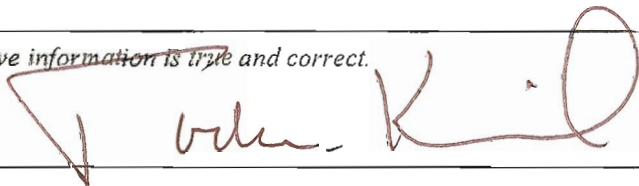
NONE

3. Please list any federal grants or contracts (including subgrants or subcontracts) received since October 1, 2010, by the entity(ies) you listed above. Include the source and amount of each grant or contract.

NONE

I certify that the above information is true and correct.

Signature:



Date:

26 SEP 14



## Todd M. Keil

Todd M. Keil has more than 27-years of experience in global security operations and management, intelligence and law enforcement, and threat assessment and risk mitigation in the government and the private sector. He is currently a Senior Advisor at TorchStone Page, LLC, providing world-leading individuals and organizations with end-to-end risk avoidance solutions.

Mr. Keil was appointed in December 2009 by President Barack Obama as the Assistant Secretary for Infrastructure Protection at the U.S. Department of Homeland Security. His office was responsible for protecting the assets of the United States essential to the nation's security, public health and safety, economic vitality, and way of life. These assets are divided into 18 separate sectors as diverse as critical manufacturing, banking and finance, commercial facilities and information technology. Mr. Keil served in this position until February 2012. Prior to his appointment, Mr. Keil worked in corporate security management positions at Texas Instruments, Inc., and the Welsh-Sullivan Group, LLC.

Mr. Keil also held numerous key positions at the U.S. Department of State's Diplomatic Security Service over 22-years of service, culminating his career as the Regional Director for Western Hemisphere Affairs, where he championed protection of U.S. government facilities, personnel, and national security information. In Foreign Service positions at U.S. embassies in Indonesia, Ireland, and Austria, he provided a broad range of security and law enforcement management and risk mitigation expertise advising U.S. ambassadors, and in primary liaison roles with a wide network of global law enforcement, intelligence, and security agencies. From 1994 to 2000, he held a leadership position on the protective detail that provided personal protection for two Secretaries of State.

Mr. Keil possesses a unique blend of field and high-level management skills and contacts, combined with his expertise in law enforcement, threat and risk assessment and mitigation, and applying business best practices in the private sector and to government operations.

Mr. Keil holds a Bachelor of Arts in Political Science and Criminal Justice from Ripon College in Ripon, Wisconsin. He has also attended special studies programs at the University of Bonn in Germany and the American University in Washington, D.C.