Testimony of Richard F. Wilson

Lieutenant of Police, Dallas Police Department, Dallas, Texas

Director of the Dallas Fusion Center

Before the

U.S. House of Representatives

Committee on Homeland Security

Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies

Austin College, Sherman, Texas

April 7, 2016

Chairman Ratcliffe, Ranking Member Richmond, members of the Subcommittee, thank you for the opportunity to testify today.

The challenges faced by law enforcement at the local level in preparing for and preventing cyber attacks are on the rise, and continue to be difficult. While all Americans recognize our dependence on the internet and telecommunication devices to stay connected with the world, this increasing level of connectivity has resulted in additional responsibilities for public officials and law enforcement to police the worldwide communications network without impeding communications between all members of their community.

The first and perhaps most difficult challenge the Dallas Police Department and our community partners face today, is our total reliance on computer networks for operational and investigative functions. This all-inclusive dependence allows for a much greater negative impact on our abilities to perform our duties when these systems fail or become infected.

Second, the extent of this connectivity enables persons and organizations with malicious intent to conduct cyber attacks from greater distances. This ability for a hacker to attack systems worldwide expands the list of possible suspects to all of the world's population that possess a smartphone or computer connected to the internet.

Third, the quantity of information passing through all communications networks allows hackers to avoid the trained systems analysts, and target their attacks to enter networks at their weakest points, by exploiting lapses in security committed by end users or consumers.

Since cyber attacks recognize no state and local jurisdictional boundaries, public officials and corporate managers must coordinate their investigative and management processes to define roles for all partners.

The pace at which technology continues to advance is currently outpacing law enforcement's ability to educate its workforce to recognize and address cybercrime activity. For those officials that do recognize the necessity to increase security infrastructures, and choose to develop or subscribe to cyber protection programs, the costs associated with these efforts often compete with funds required to maintain other essential tasks within the organizations, where the impact from these other functions can be more readily counted and observed by such measures as crime rates and response times to calls for service.

For those state and local agencies that commit funds for hiring cyber trained personnel, these agencies are often unable to compete financially with compensation packages and programs offered by private corporations and federal agencies.

Lastly, while most state and local agencies recognize their need to enhance cyber training for their existing workforce, the growing demand for cybersecurity and cyber investigative training far exceeds the current class sizes and training opportunities.

Cyber training is an expanding area of instruction that often provides training to state and local partners at reduced costs or without tuition. While these programs reduce the direct costs of obtaining training for state, local, and tribal employees, some indirect costs may result from committing a portion of the workforce to training. The student employee's absence can produce temporary staffing shortages that may adversely affect the employer agency's responsiveness to calls for service, visual presence and enforcement activity in the community, and the ability to conduct timely investigations of reported crimes.

Due to the size and mission of the Dallas Police Department, and the wide range of assignment based duties performed by DPD officers and civilians, supervisors within each division or unit are responsible for identifying job specific training needs beyond state mandated training requirements, and obtaining instruction for all employees within their workgroup.

Currently, a variety of onsite cyber training courses are offered by organizations such as the Federal Law Enforcement Training Center in Georgia, the National Computer Forensics Institute in Alabama, and Abbott Laboratories in Illinois. Some examples of additional training that can be obtained online are, SEARCH Online training and at the National White Collar Crime Center. There are also additional training and support programs offered by other DHS components FEMA and ICE, as well as the Multi-State Information Sharing & Analysis Center.

While detectives and analysts from the Dallas Fusion Center have been able to attend some of these training programs, there are always challenges for a first responder organization like the Dallas Police Department.

As such, our core capabilities at the Dallas Fusion Center are always subject to staffing patterns, personnel changes, and other policy considerations, so that to keep our level of current cyber expertise consistent and on the cutting edge, we need affordable access to cost-effective and timely training to stay on the vanguard.

Having said that, I think we can all agree that this challenge is one we face as a nation, and not just in a select few states, regions, or cities.

It will take a full-time training effort and identified funding resources for the first responders of the Dallas Police Department, and other major metropolitan cities across the country, to stay current in our struggle to meet the increasing sophistication of cybercrime, especially in today's threat landscape.

While much progress has been made in identifying the needs of state, local, tribal, and territorial agencies to address illegal cyber activity, opportunities to create cyber preparedness and responsiveness at the local level do still exist.

The first area of support should be to provide increased scholarship support of formal education programs that contain emphasis on cyber security and cyber forensics. Funding for training is always an issue in the budgets of state, local, and tribal agencies.

Second, education and public service announcements should be developed and communicated by all levels of government to all Americans, to clarify the importance of each citizen's role and responsibilities for creating a safer cyber network. This type of community outreach should emphasize the importance of hardening computer systems, and provide tips for using technology in ways that reduce opportunities for computer hackers and criminals who benefit from security lapses.

Third, until the gap between training opportunities supply is reduced to match the increasing need for training, additional facilities and programs should be created to provide training to state, local and tribal government employees.

Lastly, I would urge each member of congress to continue to create legislation as necessary to address emerging methods of cybercrime activity, as they are identified, and require stiff incarceration sentences for those convicted of committing cybercrimes.

Thank you again Chairman Ratcliffe and Ranking Member Richmond for the opportunity to testify before you today. I would be glad to answer any questions.