CYBER PREPAREDNESS AND RESPONSE AT THE LOCAL LEVEL

FIELD HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

APRIL 7, 2016

Serial No. 114–62

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpo.gov/fdsys/

U.S. GOVERNMENT PUBLISHING OFFICE

22–755 PDF WASHINGTON : 2016

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

MICHAEL T. MCCAUL, Texas, *Chairman*

LAMAR SMITH, Texas
PETER T. KING, New York
MIKE ROGERS, Alabama
CANDICE S. MILLER, Michigan, *Vice Chair*
JEFF DUNCAN, South Carolina
TOM MARINO, Pennsylvania
LOU BARLETTA, Pennsylvania
SCOTT PERRY, Pennsylvania
CURT CLAWSON, Florida
JOHN KATKO, New York
WILL HURD, Texas
EARL L. "BUDDY" CARTER, Georgia
MARK WALKER, North Carolina
BARRY LOUDERMILK, Georgia
MARTHA MCSALLY, Arizona
JOHN RATCLIFFE, Texas
DANIEL M. DONOVAN, JR., New York
BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
BRIAN HIGGINS, New York
CEDRIC L. RICHMOND, Louisiana
WILLIAM R. KEATING, Massachusetts
DONALD M. PAYNE, JR., New Jersey
FILEMON VELA, Texas
BONNIE WATSON COLEMAN, New Jersey
KATHLEEN M. RICE, New York
NORMA J. TORRES, California

BRENDAN P. SHIELDS, *Staff Director*
JOAN V. O'HARA, *General Counsel*
MICHAEL S. TWINCHEK, *Chief Clerk*
I. LANIER AVANT, *Minority Staff Director*

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES

JOHN RATCLIFFE, Texas, *Chairman*

PETER T. KING, New York
TOM MARINO, Pennsylvania
SCOTT PERRY, Pennsylvania
CURT CLAWSON, Florida
DANIEL M. DONOVAN, JR., New York
MICHAEL T. MCCAUL, Texas *(ex officio)*
CEDRIC L. RICHMOND, Louisiana
LORETTA SANCHEZ, California
SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
BENNIE G. THOMPSON, Mississippi *(ex officio)*

BRETT DEWITT, *Subcommittee Staff Director*
JOHN DICKHAUS, *Subcommittee Clerk*
CHRISTOPHER SCHEPIS, *Minority Subcommittee Staff Director*

CONTENTS

Page

STATEMENT

The Honorable John Ratcliffe, a Representative in Congress From the State of Texas, and Chairman, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies 1

WITNESSES

Mr. Alphonse Davis, Deputy Director/Chief Operations Officer, Texas A&M Engineering Extension Service:
Oral Statement 4
Prepared Statement 6
Mr. Sam Greif, Chief, Plano Fire-Rescue Department, Plano, Texas:
Oral Statement 7
Prepared Statement 9
Mr. Richard F. Wilson, Lieutenant, Dallas Police Department, Dallas, Texas:
Oral Statement 11
Prepared Statement 14
Mr. Don Waddle, Detective (Ret.), Greenville Police Department, Greenville, Texas:
Oral Statement 15
Prepared Statement 17

APPENDIX

Questions From Chairman John Ratcliffe for Alphonse Davis 29
Questions From Chairman John Ratcliffe for Sam Greif 30
Questions From Chairman John Ratcliffe for Richard F. Wilson 30
Questions From Chairman John Ratcliffe for Don Waddle 30

CYBER PREPAREDNESS AND RESPONSE AT THE LOCAL LEVEL

Thursday, April 7, 2016

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES,
Sherman, TX.

The subcommittee met, pursuant to call, at 11:09 a.m., in the Mabee Foundation Banquet Room, Wright Campus Center, Austin College, 1301 East Brockett, Sherman, Texas, Hon. John Ratcliffe [Chairman of the subcommittee] presiding.

Present: Representative Ratcliffe.

Also present: Representative Burgess.

Mr. RATCLIFFE. Good morning. The Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies will come to order.

The subcommittee is meeting today to learn how State and local officials prepare for, respond to, and investigate cyber incidents, and to learn about different cyber training opportunities for State and local officials to bolster our cyber preparedness and response.

I appreciate the effort taken by everyone that is involved here to put together an important field hearing. I would like to start by thanking our friends here at Austin College for letting us hold this hearing today here at the Mabee Hall.

This is an official Congressional hearing, as opposed to a town hall meeting, and, as such, there are certain rules of the Committee on Homeland Security and the House of Representatives that we have to abide by. So for our guests here today, we can't have demonstrations from the audience, including applause, verbal outbursts, the use of signs or placards. All those things, as fun as they may sound, are a violation of the rules of the House of Representatives. It is important that we do respect the decorum and rules of the committee, and I have also been requested to say that photography and cameras are limited to accredited press only and can't be used for campaign or political purposes.

As Americans become more aware every single day as they turn on their computers and their televisions, cyber threats are exponentially increasing. They come from criminal organizations, nation states like China, Russia, and Iran, and even terrorist groups like ISIS. These attackers don't only target Federal networks, big banks, and National retail chains. They also hit towns and families and local businesses. So there is a great need to address cybersecurity at the State and local level.

From emergency response centers, Department of Motor Vehicle offices, to courthouses and our critical infrastructure, the exploitable vulnerabilities and possible consequences for public safety are alarming. On the law enforcement side, FBI Director Jim Comey recently testified that an element of virtually every National security threat and crime problem that the FBI faces is cyber-based or facilitated. It is incredible that Federal law enforcement is seeing a cyber element to almost every single crime.

Because society is increasingly connected, we can be certain that our State and local law enforcement are seeing the same trend, arguably with even fewer tools to address it. It no longer takes a sophisticated cyber criminal to compromise sensitive information from companies and from everyday Americans, and law enforcement is seeing a cyber element to almost every crime. It is vital that State and local law enforcement, the prosecutors and judges all be properly trained to respond to cyber crime and to protect the American people.

We have recently seen a flurry of ransomware attacks against hospitals, including at least one located here in the 4th Congressional District of Texas, where patients' personal medical data is encrypted and held hostage until the hospital pays a ransom to get it back. As reports indicate, cyber attacks against emergency workers are spiking and will continue to rise.

We all recognize that interconnectivity and automation increase convenience and improve responses. Emergency services are just one area where automation and interconnectivity provide clear benefits to us all. But while these technologies increase efficiency and cut costs, they do present new risks that, if exploited, could bring vital emergency services and our critical infrastructure to a halt.

Regardless of the magnitude of a natural or man-made disaster, first responders—firemen, police, paramedics, and National Guardsmen—are the ones, the first ones that are on the scene. Their ability to communicate and to execute key command-and-control responsibilities during an incident often depends entirely on internet-enabled technologies.

As we examine cyber preparedness and response at the State and local level, I am pleased that we are joined by a number of distinguished witnesses this morning who are at the tip of the spear in this effort. I look forward to hearing about how they are preparing for, responding to, and mitigating and investigating the threats that we face right now in cyber space.

I am also pleased that this hearing is taking place not in the halls of Congress today but right here in the 4th Congressional District of Texas, the first-ever Congressional hearing here in Grayson County. The police, prosecutors, judges, paramedics, and firefighters, they all need the appropriate tools and training to respond to the increasing threats that we face, and to make sure that they are fully equipped, we need to hear directly from them. The best solutions, believe it or not, don't usually come from Washington, DC. People often hear me say that governing is a team sport, and I think that today's hearing and the location of today's hearing hopefully reinforces that fact.

As Chairman of this subcommittee, I have been closely examining these challenges. I will continue to lead efforts in Congress

to strengthen our Nation's cyber defenses and provide for the common defense against these National security threats.

Last fall, I authored and moved legislation to strengthen State and local cyber crime-fighting efforts. Specifically, the legislation would support the National Computer Forensics Institute, or NCFI, which is run by the United States Secret Service, and provides greatly-needed cyberforensics training to State and local law enforcement across the country, including those right here in Texas' 4th District. In fact, we are pleased today that one of our witnesses, former Greenville Detective Don Waddle, was trained at the NCFI.

Today I hope this subcommittee will learn more about how first responders here in Texas are being trained to address cyber incidents, how first responders are preparing for and responding to cyber incidents, and how local law enforcement officials are being trained in computer forensics.

This hearing will provide needed background to further reinforce the subcommittee's efforts regarding cyber training and workforce needs at the State and local level. Cybersecurity is a shared responsibility, including all levels of government and the private sector.

While much has been done to improve our Nation's cybersecurity, there are a number of challenges that remain. I look forward to hearing from our witnesses today as we consider ways to address those challenges.

My good friend, Mr. Burgess of Texas, is here today, and I ask unanimous consent for him to be permitted to sit and participate in today's hearing.

Without objection, so ordered.

Other committee Members are reminded that opening statements may be submitted for the record.

Before I introduce the distinguished panel of witnesses before us on this important topic today, again I would like to thank a number of folks that are here.

I mentioned Austin College President Hass, for always being a hospitable host to us.

We have a number of law enforcement folks that are here today that are not testifying.

Lieutenant McGreevy from Sherman Police Department.

From Denison Police Department we have Assistant Chief Joe Clapp, Assistant Chief Don Maury, Paris Fire Chief Larry Wright, and Assistant Chief Thomas McGonagall.

Constable Bob Douglas from Grayson County; Commissioner Jeff Whitmeyer from Grayson County; Dan Sharp from the Denison IT department; Tom Watt, a Grayson County sheriff-elect.

We have Rita Knowles, justice of the peace, who is here, Tammy Johnson from the Sherman City Council, Kevin Couch from the Sherman City Council, Reggie Smith, esteemed local activist.

We have assistant chief of the Sherman Police Department, Lieutenant John Henneberg, here. I would also like to welcome Terra Petty and Daryl Birkland from Wilson and Jones IT department.

I am sure I am leaving some others out and I apologize, but I am trying to recognize everyone who has taken the time to be here, including a number of students here from Austin College. Welcome.

Thank you for being a hospitable host to us. I would say that I have been the beneficiary personally of a number of Austin College students who have interned in my Congressional office, and a number of them are here today. Thank you for coming back. It is great to see you all again.

With that, I would like to recognize our distinguished panel of testifying witnesses this morning.

We have with us Mr. Al Davis, who is the deputy director and chief operations officer at Texas A&M Engineering Extension Service. Welcome, Mr. Davis.

Mr. DAVIS. Thank you, sir.

Mr. RATCLIFFE. We have Mr. Sam Greif, the chief of the Plano Fire-Rescue Fire Department, who is testifying on behalf of the International Association of Fire Chiefs. Welcome, Chief.

Mr. GREIF. Thank you, sir.

Mr. RATCLIFFE. We have Mr. Richard Wilson, who is a lieutenant with the Dallas Police Department. Welcome, lieutenant.

Last but not least, we have now-retired Detective Don Waddle from the Greenville Police Department.

Mr. WADDLE. Thank you, sir.

Mr. RATCLIFFE. Very good. All right.

With that, I would like to ask the witnesses to stand so that I can administer an oath.

[Witnesses sworn.]

Mr. RATCLIFFE. Let the record reflect that the witnesses have answered in the affirmative.

The witnesses' full written statements will appear in the record.

You may be seated.

The Chair now recognizes Mr. Davis for 5 minutes for his opening statement.

STATEMENT OF ALPHONSE DAVIS, DEPUTY DIRECTOR/CHIEF OPERATIONS OFFICER, TEXAS A&M ENGINEERING EXTENSION SERVICE

Mr. DAVIS. Thank you very much, Mr. Ratcliffe. I would like to thank you and also Mr. Burgess and other Members of the subcommittee. It is an honor to appear here before you on behalf of our agency, the Texas A&M Engineering Extension Service, to discuss cyber preparedness and response at the local level.

I will start by telling you just a little bit about TEEX. We are affectionately known as TEEX to those that we train and that we partner with. We began training in 1930. The impact is at the local, State, and National, and global levels. We cover training and technical assistance across the entire homeland security enterprise domain to include cybersecurity, and an important part of our mission and our role is our extension service, we are proud to say, to the great State of Texas.

Our relationships. First of all, we have relationships with responders across all disciplines, all 16 disciplines, at the State and local levels. With DHS/FEMA, we have relationships not only with the National training and education division but with CS&C, Cybersecurity and Communications, who we dialogue with. We also dialogue with the Infrastructure Protection Directorate, Personal Protection Directorate, and the Office of Bombing Prevention.

We also have consortium memberships, first of all, since 1998, with the National Domestic Preparedness Consortium, with the National Cybersecurity Preparedness Consortium, and we are also a member of the Forensics Consortium. Those memberships help us to address cybersecurity across a number of areas.

Our role in addressing the cybersecurity challenge began in 2010 when DHS/FEMA asked us to take on some training that was previously done on a competitive training grant. We have also linked cybersecurity to emergency planning and response, and we think that is very, very important.

Why we think it is important: I think the police chiefs and fire chiefs would agree, we used to think about cybersecurity on the left hand and emergency planning and response on the right hand, and they should be thought about together, because if the emergency response planner or manager thinks that they can really put off a plan or respond without cyber intrusion, that is not accurate. That is really not accurate because of those reasons you stated, sir.

We have done some pioneering efforts also, and what I mean by that is when we visit a lot with our partners at DHS/FEMA, we didn't visit in silos. We thought there was a need to bring them together, and we are proud to say that we did, in fact, bring those different entities together to actually develop further training. So again, we were pioneers in that effort.

We also at TEEX, through cybersecurity technical assistance and vulnerability assessments—that is very important, we do that not only with some universities, but we have been doing that with some communities. We have done some training also, assessments that is, in Congress, and Texas also, sir.

As far as our products go—and that is our training courses—this focuses also on training, and I will refer to something we submitted, our statement. We had 5 instructor-led courses. Four deal with cyber and incident management, and it comes from the community level, the Essentials of Community Cybersecurity, Community Preparedness, and Community Cybersecurity Exercise Planning.

We also have 10 on-line courses that are provided at no cost to individuals, designed for 3 levels of students, including the general user, which is very important—you addressed that, sir—the information technology staff and specialists, and for business managers also. So again, that training is, at no cost, available to the general public.

As far as our results, over the last 5 years TEEX has provided cybersecurity training for students and participants in 40 States and 5 territories, reaching a total of 32,900 training instances, and we think that is very, very important.

As we move forward, sir, we will continue to work closely with States and local communities in identifying their needs and supporting their efforts. States have reported, through the National Preparedness Reports beginning in 2012, that cybersecurity is a key National area of improvement and concern, and it is listed as a top priority in the 2014 and 2015 National Preparedness Report.

So again, we are very, very pleased to be here. We have submitted a statement in more detail, and I will be willing, sir, when appropriate, to take your questions that you may have.

[The prepared statement of Mr. Davis follows:]

PREPARED STATEMENT OF ALPHONSE DAVIS

APRIL 7, 2016

Chairman Ratcliffe, and other distinguished Members of the subcommittee, it is an honor to appear before you today on behalf of the Texas A&M Engineering Extension Service (TEEX) to discuss cyber preparedness and response at the local level.

HISTORY OF TEEX EMERGENCY MANAGEMENT TRAINING PROGRAM

TEEX, a State of Texas agency and member of the Texas A&M University System (TAMUS), began training State and local responders in 1930, and today trains over 170,000 annually from across the world. In 1998, TEEX became a founding member of the National Domestic Preparedness Consortium (NDPC). The NDPC is a partnership of 7 universities and organizations that are the primary means through which the Department of Homeland Security/Federal Emergency Management Agency's (DHS/FEMA) National Training and Education Division (NTED) provides training to State, local, Tribal, and territorial responders and communities in support of PPD–8—National Preparedness. The NDPC is Congressionally-authorized and annually appropriated funding through the Homeland Security National Training Program to develop and deliver training for the Nation's emergency first responders within the context of all hazards; including chemical, biological, radiological, and explosive Weapons of Mass Destruction (WMD) hazards. To date the NDPC has trained over 2.4 million, more than 540,000 of which were trained by TEEX.

This long-term relationship with State and local level emergency managers, responders, and leaders, and infrastructure/industrial partners, along with more than 20 years of experience in workforce and software development, prepared TEEX to provide training on preparedness and response for cyber incidents or attacks. In today's connected world cyber refers to anything that contains, is connected to, or is controlled by computers and computer networks.

BEGINNING OF TEEX CYBER TRAINING PROGRAM

In 2010, at the request of FEMA, TEEX began training State and local communities in cybersecurity awareness, specifically where local communities and responders need to collaborate with their critical infrastructure partners in planning for and responding to a possible cyber attack or incident. TEEX launched this effort within their existing HSNTP funding (then fiscal year 2009—$22,344,500) by continuing the delivery and maintenance of cyber courses originally developed under FEMA Continuing Training Grants and awarded to other universities.

At the National level, the need for an increase in cybersecurity awareness and the ability to collaboratively plan with critical infrastructure partners was highlighted through PPD–21—Critical Infrastructure Security and Resilience and EO–13636—Executive Order Cybersecurity/Presidential Policy Directive on Critical Infrastructure Security and Resilience. TEEX responded to the growing need by expanding the cyber training program and leveraging the partnerships with the DHS Office of Infrastructure Protection (IP) and the DHS Office of Cybersecurity and Communications (CS&C). TEEX had previously developed 2 courses on the protection of critical infrastructure with DHS/IP and was asked to develop a third, which specifically-focused on the challenges of both physical and cybersecurity on critical infrastructure, with DHS/IP and DHS/CS&C.

CURRENT TEEX TRAINING AND ASSESSMENT PROGRAMS

TEEX trains students through the DHS/FEMA HSNTP, offered at no cost to State, local, Tribal, and territorial communities, and includes:

- 5 instructor-led courses that are delivered across the country and the U.S. territories, allowing communities to train together in the classroom:
  - 4 courses on cyber and incident management
    - Promoting Community Cybersecurity
    - Essentials of Community Cybersecurity
    - Community Preparedness for Cyber Incidents
    - Community Cybersecurity Exercise Planning.
  - 1 course specifically addressing both physical and cybersecurity
    - Physical and Cybersecurity for Critical Infrastructure.

- 10 on-line courses, available at no cost to individuals, designed for 3 levels of student, including:
  - 3 courses for General Users, covering broadly-applicable awareness needs
  - 4 course for Information Technology staff and specialists, addressing security, forensics, and response techniques for IT systems
  - 3 courses for Business Management staff that include Risk Management and legal parameters critical to small businesses.

In addition to training, TEEX also provides technical assistance, offering community and organizational vulnerability assessments and compliance reviews. Vulnerability assessments include network vulnerability testing, review and validate IT security processes, and review IT system security configurations, while compliance reviews include organizational policy conformance reports and recommendations to make their systems more secure.

IMPLEMENTATION OF TEEX TRAINING PROGRAMS

Over the last 5 years, TEEX has provided cybersecurity training for students in 40 States and 5 territories, reaching a total of 32,290 students. These students trained both in the classroom and on-line.

- Instructor-led training (delivered in local communities):
  - 345 deliveries to 8,413 students in the United States
  - 31 deliveries to 815 students in Texas.
- Online training:
  - 23,877 students in the United States
  - 4,264 students in Texas
  - 50 students in TX District 4.

FUTURE OF TEEX TRAINING PROGRAMS

As we move forward, we will continue to work closely with States and local communities in identifying their needs and supporting their efforts. States have reported through the annual National Preparedness Reports, beginning in 2012, that cybersecurity is a key National area of improvement, listing it as a top priority in 2014 and 2015. Some of our recent work in support of the States includes:

- Working with States to provide employee training web portals with direct access to State-identified required on-line cyber training and reporting capabilities for States to monitor employee progress in completing the courses. Student training portals are now active for the States of Arkansas, Louisiana, and Wyoming, as well as Fresno Pacific University in California.
- Most recently, as a member of the National Cybersecurity Preparedness Consortium (NCPC), consisting of 5 partners focused on training for State and local communities, TEEX is developing new training on the integration of cybersecurity into the local Emergency Operations Center (EOC). Through FEMA NTED's Continuing Training Grants, TEEX will develop 2 hands-on courses, with simulated scenarios designed to develop managerial and operational-level skills sets. The first course, now in development and piloted in Utah and Rhode Island, is designed to help ensure that traditional emergency management personnel and IT personnel recognize the importance of working together to mitigate the effects of a cyber incident. A second, more technical, course will follow and will provide students with the key skills and processes needed to more effectively defend their organizational networks.

In summary, we will continue to focus on how we can further assist and prepare local entities for a cyber incident, as well as enhancing engagement with the public and private sectors in planning and response to a cyber incident.

Mr. RATCLIFFE. Thank you, Mr. Davis.

The Chair now recognizes Chief Greif for his opening statement.

STATEMENT OF SAM GREIF, CHIEF, PLANO FIRE-RESCUE DEPARTMENT, PLANO, TEXAS

Mr. GREIF. Good morning, Chairman Ratcliffe, Representative Burgess. Today I thank you for the opportunity to represent the International Association of Fire Chiefs to discuss this important topic.

Cyber crime and cyber attacks are an ever-increasing threat to the American homeland. However, fire and emergency services are

still learning how to recognize these threats and the adverse effects of those to our operations. There have been attempts to use robocalls and other service attacks that would affect operations of 9–1–1 public safety answering points. In addition, we have seen recent examples of cyber attacks against hospitals in California, Kentucky, and the Washington, DC area.

The greater concern is that a cyber attack can be used in conjunction with kinetic bombing or an active-shooter incident to create confusion during the response. Fire and EMS departments must be vigilant for malware, phishing, spam, spyware, and other new and diverse threats. The keys to successful cybersecurity efforts for fire and EMS departments are multifaceted.

We need to harden and test systems, stay aware of and informed by our new threats, and make sure that the staff are trained and prepared to prevent and to respond to a cyber incident. It is vital that fire and EMS departments take steps to protect themselves.

During my tenure with the Fort Worth Fire Department, I oversaw our Fire Communications Division. In order to protect our computer-aided dispatch and 9–1–1 systems, IT departments segregated them from the outside world. This reduced their vulnerability. We updated the systems by testing updates and manually installing them on our servers.

To protect the PSAPs, departments have to constantly test the 9–1–1 system vulnerabilities to make sure that they can withstand a concerted service attack. PSAPs also should be constructed securely from the outside attacks and have resilient systems as backup.

As public safety communications move to digital systems, they can become vulnerable to cyber attacks. These communication systems must be secured. Fire and EMS departments also must stay aware of new threats. State and local fusion centers can provide information about cyber threats. In addition, Federal information-sharing systems like the Homeland Security Information Network are good sources of cyber information for fire and EMS chiefs.

Fire and EMS chiefs also should develop close working relationships with their local law enforcement, emergency managers, IT departments, and the surrounding jurisdictions. At Fort Worth, I worked with the local police and intelligence communities to stay aware of these threats. In Plano, I meet monthly with the police chief, the public safety communications director, the emergency management director, and among our discussions is how to improve and secure our communications systems.

Major events require regional planning. For Super Bowl XLV in 2011, we developed a multi-county consortium and developed a communications plan that actually included response to cyber terrorism.

Finally, training and exercises are key to preventing and responding to an incident. Antivirus software must be kept up-to-date. Staff should adopt preparedness and a culture to not put on any links to malware, spyware, or other threats. Fire and EMS chiefs also can study the effects of cyber attacks and other public safety and private organizations and learn how to mitigate the consequences before they occur.

The Federal Government can be an important partner in a Federal cybersecurity regime. Many fire departments are not aware of the threat that they face. DHS can work with the U.S. Fire Administration and the National Fire Academy to develop standards and training for all fire and EMS departments. Fire chiefs recommend that the U.S. Fire Administration's budget be restored to the fiscal level of 2011, which was $45.6 million, in order to facilitate this type of educational effort. In addition, DHS can continue to fund the State Homeland Security Grant Program and the Urban Area Security Initiative, also known as UASI. These programs support their operations. In addition, these grants can be used to fund cyber components to regional training. Unfortunately, the administration's fiscal year 2017 budget request would impose Draconian cuts on these programs. The State Homeland Security Grant Program will be cut by more than 50 percent, and the UASI program would be cut by 45 percent. We recommend that these programs be funded at least to the fiscal year 2016 level of $467 million for State Homeland Security Grant Program and $600 million for UASI.

Thank you for the opportunity to represent Fire and Emergency Services at today's hearing. Local fire and EMS departments must take necessary precautions to protect themselves from this new and emerging threat. In addition, the Federal Government can provide critical information, education, and practical training about the threat of cyber attacks.

I look forward to answering any questions you may have.

[The prepared statement of Mr. Greif follows:]

PREPARED STATEMENT OF SAM GREIF

APRIL 7, 2016

Good morning, Chairman Ratcliffe, Ranking Member Richmond, and Members of the subcommittee. I am Chief Sam Greif of the Plano Fire-Rescue Department. Today I am pleased to testify on behalf of the International Association of Fire Chiefs. The IAFC represents more than 11,000 leaders of the Nation's fire, rescue, and emergency medical services. Thank you for the opportunity to discuss important issues related to cybersecurity and the fire and emergency service. This is a growing threat that adds yet another mission for the America's firefighters and emergency medical personnel.

THE PROBLEM OF CYBERSECURITY

Cyber crime and cyber attacks are becoming a more prevalent threat to the American homeland. A 2010 report by Norton found that two-thirds of the world's population have been the victim of some form of cyber crime. A 2009 study by McAfee demonstrated that cyber crime, including security breaches and data theft, may have cost international business has much as $1 trillion. We have seen how cyber attacks can harm major universities, medical facilities, financial institutions, retailers, local governments, and Federal agencies.

The fire and emergency service is just beginning to recognize how these threats can affect our operations. There have been attempts to use robocalls and other denial-of-service attacks to affect operations at 9–1–1 Public Safety Answering Points (PSAP). Just recently, we have seen a rash of cyber attacks against hospitals in California, Kentucky, and the Washington, DC area. In addition, we always must be vigilant for malware, phishing, spammers, and spyware which are aimed at infiltrating and debilitating our systems.

From the fire and emergency service's perspective, it is important that we protect vital systems that support our operations. The 9–1–1 systems are necessary for the public to call and request assistance during emergency situations. Computer-aided dispatch (CAD) systems are essential for determining which units are available to respond and assigning them to an incident scene. These units must be able to com-

municate with the dispatch center, command units and each other effectively at the incident scene. In addition, patient reporting information must be protected by the emergency medical service (EMS), because of the nature of the data. As the Nation transforms to a more digital world and the "Internet of Things," all of these capabilities will be presented with an increasing number of opportunities to provide service to our citizens and a corresponding number of vulnerabilities to cyber threats.

PROTECTING THE FIRE AND EMERGENCY SERVICE

As they consider the various threats to their computer systems, fire and EMS departments must take steps to protect themselves. Before I became fire chief in Plano, I served for 30 years in the Fort Worth Fire Department, where I oversaw the city's 9–1–1 center for 10 years. One of our major missions was to protect our CAD and 9–1–1 systems from cyber attacks. To protect our systems, we segregated them from the outside world. This action minimized the ability of outsiders to compromise our systems through the internet. To update our systems, we would have to go to the server and install software manually. It is important to recognize, though, that most of a fire and EMS department's computer systems, like human resources, email, and finance, will be part of the overall jurisdiction's information technology (IT) systems.

Fire and EMS departments also have to take steps to harden their systems. In order to protect their 9–1–1 systems from massed robocalls aimed at taking down the system, the departments have to constantly test their systems' vulnerabilities to make sure that they can withstand heavy call volumes. The fire departments also have to download and use a testbed to evaluate all software before installing it. It is important to realize that—as communications systems move to digital systems that use VoIP—these systems need to be secure from cyber attacks that might compromise life-saving operations on the fire scene. In addition, 9–1–1 Public Safety Answering Points (PSAP) should be constructed to be secure from outside attacks and have resilient systems and back-up power.

As with other threats, local fire and EMS chiefs must stay aware of new threats and prepare for them. The best way to stay informed is to develop relationships with intelligence fusion centers, Federal officials and local law enforcement. If fire and EMS departments can support the staffing requirements, they should have personnel stationed at the State and local fusion centers. Grants administered by the Federal Emergency Management Agency (FEMA), including the State Homeland Security Grant Program (SHSGP) and Urban Areas Security Initiative (UASI), will support fire and emergency service personnel in fusion centers. Fire and EMS departments also should maintain close relationships with local Joint Terrorism Task Forces. These resources will keep fire and EMS chiefs informed on the latest cyber threats and help them address any vulnerabilities.

It also is important to develop close working relationships with local law enforcement officials. In Fort Worth, I worked with the local police intelligence unit, which was aware of new threats to the community. In Plano, the public safety group, composed of the city communications director, the police chief, the emergency manager and me, meet monthly to discuss threats and how to prepare for them.

Federal information-sharing systems, like the Homeland Security Information Network (HSIN), also can provide important information about cyber threats and how to prepare for them. HSIN is a National, secure, web-based portal for information sharing and collaboration between Federal, State, local, Tribal, territorial, and private-sector partners. HSIN has a community of interest dedicated to the fire and emergency service. The U.S. Department of Homeland Security (DHS) must make sure that cybersecurity-related information is added to this community of interest, so that local fire and EMS chiefs can access it.

Since fire and EMS departments depend on mutual aid to respond to major incidents, they should address cybersecurity concerns as part of their planning and training. Communications must be interoperable during an incident; a breakdown in communications or dispatch systems during an incident could cause confusion at a critical time. To address this risk, the North Central Texas Council of Governments addressed cybersecurity as part of its interoperability plans. For Super Bowl XLV in 2011, the Multi-Quad County Consortium developed a communications plan that addressed cybersecurity concerns and developed plans for responding to a cyber attack.

Finally, training and exercises are key to preventing and responding to an incident. One of the basic ways to protect computer systems is to train staff not to click on spamware, malware, or spoofing attacks. In addition, fire and EMS departments must ensure that all of their virus software is up-to-date. These are simple tasks that can protect a system. Fire and EMS departments also can audit their systems

to evaluate vulnerabilities. It also is worthwhile to study the effects of cyber attacks on other public safety organizations to see how their operations were affected and what they did to mitigate the damage. Local fire and EMS departments can work with local law enforcement agencies, emergency managers and the jurisdictions' IT staff to plan and exercise contingency plans in case of cyber attacks aimed at taking down key systems.

THE FEDERAL GOVERNMENT'S ROLE

The Federal Government can be an important partner. Most importantly, it can help educate fire and EMS departments about the cybersecurity threat. The DHS's Office of Cybersecurity and Communications (C&SC) can work with FEMA to raise awareness in local fire departments about the threats that cyber attacks can pose. The U.S. Fire Administration (USFA) is an agency within FEMA that supports the local fire and emergency service. By working with USFA and its National Fire Academy, C&SC can develop education and training to help fire and EMS departments learn how to determine which systems might be vulnerable to cyber attacks and make the necessary changes to protect them. It is important to note that the President's fiscal year 2017 budget proposes to cut USFA by $1.7 million. We recommend that—instead—Congress fund USFA at the fiscal year 2011 level of $45.6 million, so that the agency can develop training for emerging threats like cybersecurity.

Also, DHS can continue to support training and exercises to help fire and EMS departments prepare for the threat of a cyber attack. A cyber-related component can be added to the State and local exercises. In addition, DHS should continue to support State and local fusion centers, which serve an important purpose in sharing threat information. These programs are funded though the SHSGP and UASI programs. Unfortunately, the President's fiscal year 2017 budget proposes to cut these programs drastically. The budget would cut the SHSGP program to $200 million (a decrease of more than 50%) and the UASI program would be cut to $330 million (a 45% cut). We urge Congress to fund these programs—at least—at the fiscal year 2016 level of $467 million for the SHSGP program and $600 million for the UASI program.

Recently, the DHS National Protection and Programs Directorate (NPPD) announced a proposal to realign itself to have a greater focus on cybersecurity. Overall, the IAFC is supportive of this proposal. However, we have concerns about how this realignment would affect the Office of Emergency Communications (OEC). The OEC's mission is to promote public safety communications interoperability using a local stakeholder-directed approach. The IAFC and other public safety organizations do not support efforts to move OEC under the Infrastructure Security component. Instead, we recommend that OEC remain a separate component within NPPD.

CONCLUSION

Thank you for the opportunity to testify at today's hearing. Cybersecurity is an issue of growing importance to the Nation. A breakdown of a fire and EMS department's CAD or communications system during the response to an incident could result in tragic consequences. It is important that local fire and EMS departments strengthen their systems to protect them. In addition, fire and EMS chiefs should develop strong working relationships with Federal, State, and local law enforcement officials to be aware of emerging threats. Finally, local fire and EMS chiefs should make sure that their staff are trained in basic cybersecurity safety, and plan and exercise for the consequences of a successful cyber attack. Taking these necessary precautions should help local fire and EMS departments to adapt to this emerging threat.

Mr. RATCLIFFE. Thank you, Chief Greif.

The Chair now recognizes Lieutenant Wilson for his opening statement.

STATEMENT OF RICHARD F. WILSON, LIEUTENANT, DALLAS POLICE DEPARTMENT, DALLAS, TEXAS

Mr. WILSON. Good morning, sir. Chairman Ratcliffe, Mr. Burgess, thank you and Ranking Member Richmond 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 con-

tinue to be difficult. While all Americans recognize our dependence on the internet and telecommunications 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 world-wide communications network without impeding communications between the members of our 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 world-wide expands the list of possible suspects to all of the world's population that possess a smartphone or computer that is 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 the partners.

The pace at which technology continues to advance is currently outpacing law enforcement's ability to educate its workforce to recognize and address cyber crime 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 on-site 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 on-line are SEARCH On-line 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 and 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 cyber crime, 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 do still exist to create cyber preparedness and responsiveness at the local level.

The first area of support should be to provide increased scholarship support of formal education programs that contain emphasis on cybersecurity 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.

Last, I would urge each Member of Congress to continue to create legislation as necessary to address emerging methods of cyber crime activity as they are identified and require stiff incarceration sentences for those convicted of committing cyber crimes.

Thank you again, Chairman Ratcliffe and Mr. Burgess, for the opportunity to testify before you today. I would be glad to answer any questions.

[The prepared statement of Mr. Wilson follows:]

PREPARED STATEMENT OF RICHARD F. WILSON

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 world-wide 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 world-wide 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 cyber crime 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 on-site 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 on-line are, SEARCH On-line 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 cyber crime, 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 cybersecurity 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.

Last, I would urge each Member of Congress to continue to create legislation as necessary to address emerging methods of cyber crime activity, as they are identified, and require stiff incarceration sentences for those convicted of committing cyber crimes.

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.

Mr. RATCLIFFE. Thank you, Lieutenant Wilson.

The Chair now recognizes Detective Waddle for his opening statement.

STATEMENT OF DON WADDLE, DETECTIVE (RET.), GREENVILLE POLICE DEPARTMENT, GREENVILLE, TEXAS

Mr. WADDLE. Good morning, Chairman Ratcliffe and Mr. Burgess. I thank you for the opportunity to speak with you all today.

I served as a police officer in both the military and civilian police departments for 39 years. The last 25 years were spent with the Greenville Police Department in Greenville, Texas. The last 15 years I was also assigned to the Criminal Investigation Division working property crimes and fraud. Fraud often involves the use of computers to facilitate those crimes. Checks are generated and printed on computers. Credit card abuse and identity theft are often committed using the internet.

I did retire from law enforcement on the 31st of last month and am now trying to settle into the quiet life.

During the last 10 years I have also been assigned to the North Texas Electronic Crimes Task Force with the United States Secret Service and worked side-by-side with both special agents of the Secret Service and with numerous State and local investigators. We were all trained to recover evidence from computers and cell phones, and we do these examinations from agencies throughout North Texas. These cases involve anything from fraud, to narcotics, to child pornography, to murder, and capital murder. I have testified in trials from possession of child pornography, to enticing a child, to murder, and capital murder.

As I look back at my career in law enforcement, I remember going to a call for a burglary, throwing some dust around and hoping that the perpetrators didn't get guns or the victims' checkbooks or credit cards. As time moved forward, computers and cell phones came into the game, and then my concern was, did they get the victims' computer passwords for their I-pads or their cell phones? It was obvious to me that for me to provide better service to the people of my city, I had to know how to catch the criminals and what they were doing, and what I needed to do to be able to present a case that would put these criminals in jail.

Computer crime investigation is not an inexpensive pursuit. All of the software programs that you use for investigations are all very expensive. All of them have licenses that have to be renewed every year, and the monetary cost to a city of my size can be anywhere from $300 a year to tens of thousands of dollars a year for the software and equipment to do these investigations.

We needed help. There was no way that we were going to be able to do that. That is where the Secret Service and Federal Government stepped in. They helped us help our citizens by providing us with training, equipment, and expertise. Because of the training I received, I became a more valuable asset to my department. I was sought out by other detectives for help with their investigations. In major crimes I have used the training I have received to assist with murder investigations by mapping out locations perpetrators used to hide their victims' bodies, or to helping detectives plot computer searches that outlined their case to intelligence for narcotics investigators.

I am also called on to assist other local agencies with their investigations. They have used the information I provided to prepare their cases for prosecution. I am also called on by the prosecutors to answer questions regarding computer crime. Had I not had this training, I would not have made the new contacts that I had that have been very beneficial to me.

In early 2006 I went to the United States Secret Service office, the Dallas field office, to drop off a computer for examination. I knew nothing about computers at that time. I spoke with Bob Sheffield, who was the head of the Electronic Crimes Special Agent Program there in the Dallas field office and the North Texas Electronic Crimes Task Force at the Dallas field office, and was telling him how interested I was in learning about forensics. He plainly said, "We can do that for you." I went to the Federal Law Enforcement Training Center in Brunswick, Georgia for 6 weeks learning about computers and computer forensics. This was prior to the National Computer Forensics Institute.

In that training I learned what a computer was, what the programs on a computer were, what their purposes were, and the overall operation of the computer, and I learned how to look for evidence of a crime.

After that I went to the National Computer Forensics Institute in Hoover, Alabama. I started to go to the training there. I went to Advanced Forensics Training there. I went to the first class, which was one of the very first classes at the Institute of any kind, so there was a little bit of tweaking that needed to be done, and then I went back and learned a great deal that helped me towards my computer forensics.

I also went to the Mobile Device Data Recovery school, or MDDR, which is cell phone training, and also just this last February went to Mac Forensic Training at the NCFI. The NCFI has worked very hard to give State and local officers like me a good, quality education and lots of tools for my toolbox and are always there to answer questions. I can call up there at any time if I have a question about something, and there is just somebody there who is going to be able to answer that question.

The instructors that they have are all very expert in their field, and they work very hard to provide all of us with the proper training that we need to be able to do our jobs. You don't have to be on a level way above our heads to talk to us.

I think that probably the best training that I ever received in my 39 years of law enforcement was there at NCFI. I walked away from each class very confident in what I had learned and was able to put all those things back into practice and was able to do those things, and I am grateful for that. I am grateful to the Federal Government for providing that kind of tool.

I would encourage giving thought to increasing the size of those classes that were offered at the facility because cyber crime is not going to do anything but increase. I have 2 trials coming up later this month that come from the investigations and the training that I got from the NCFI.

I want to thank you for your time today.

Oh, one other thing I wanted to say is that I am grateful for the training that I received, but my citizens have been the major benefactors of that training because I was able to do a better job for them.

The other thing I really liked about NCFI is that they didn't just work with law enforcement officers. They also work with judges and prosecutors to help them understand about cyber crime and what is happening there so they are able to do their jobs more efficiently, too.

I am thankful for the time that you all have given me to talk today, and I appreciate the opportunity that I have to say something about this.

[The prepared statement of Mr. Waddle follows:]

PREPARED STATEMENT OF DON WADDLE

APRIL 7, 2016

I served as a police officer in both military police and civilian police departments for 39 years. The last 25 years were spent with the Greenville Police Department in Greenville, Texas. The last 15 years I was assigned to the Criminal Investigation

Division working Property Crimes and Fraud. Fraud often involves the use of computers to facilitate the crime. Checks are generated and printed on computers. Credit card abuse and identity theft are often committed using the internet. I retired from law enforcement on March 31, 2016. During the last 10 years I have also been assigned to the North Texas Electronic Crimes Task Force with the United States Secret Service in Dallas, Texas. In this assignment I have worked side-by-side with special agents of the Secret Service and with numerous State and local investigators. We are all trained to recover evidence from computers and cell phones, and we do these examinations from agencies throughout North Texas. These cases involve anything from fraud to narcotics to child pornography to murder and capital murder. I have testified in trials from possession of child pornography, to enticing a child, to murder and capital murder.

As I look back at my career in law enforcement, I remember going to a call for a burglary, throwing some dust around and hoping that the perpetrators didn't get guns or the victims checkbook or credit cards. As time moved forward computers and cell phones came into being and on that same burglary, I now had to hope the perpetrators did not get the victims' computer passwords or their cell phones. If that happened there was no telling, how much the victim would end up being victimized. It was obvious, that for me to provide better service for the people of my city, I had to know how to catch the criminals that were committing these offenses. Computer crime investigation is not an inexpensive pursuit. The monetary cost to the city for training and equipment, can be anywhere from $300 dollars a year to tens of thousands of dollars a year. We needed help. That is where the U.S. Secret Service and Federal Government come in. They helped us help our citizens by providing us with training, equipment, and expertise. Because of the training I received, I became a more valuable asset to my department. I was sought out by other detectives for help with their investigations. In major crime I have used the training I have received to assist with murder investigations by mapping out locations perpetrators used to hide their victims bodies, to helping detectives plot computer searches that outlined their case, to intelligence for narcotics investigators. I am also called on to assist other local agencies with their investigations. They have used the information I provided to prepare their cases for prosecution. I am also called on by the prosecutors to answer questions regarding computer crime. Had I not had this training, I would not have made new contacts that could be beneficial for me as well.

In early 2006, I went to the United States Secret Service, Dallas Field Office to drop off a computer for examination. While at the office and lab, I spoke with Bob Sheffield who was the head of the Electronic Crimes Special Agent Program (ECSAP) and The North Texas Electronic Crimes Task Force (N–TEC) at the Dallas Field Office, and was telling him how interested I was in learning about forensics. Mr. Sheffield plainly stated "We can do that for you." I went to the Federal Law Enforcement Training Center in Brunswick Georgia, for 6 weeks learning about computers and computer forensics. Shortly after completing this training the National Computer Forensics Institute (NCFI) was opened in Hoover, Alabama. I started to go to the training at NCFI, and have been to Advanced Forensics Training (AFT), Mobile Device Data Recovery (MDDR) cell phone training, and Mac Forensic Training. The NCFI has a solid outline of what is needed for each class. They strive hard to provide very qualified instructors, who make every effort to give each student all they need to be qualified to do their job. The equipment NCFI provides and the equipment used for the classes is some of the very best that can be used. Not only is there discussion of ways to conduct a forensic investigation but discussion also covers court procedure and testifying. I have also been to numerous conferences related to electronic crime and have always come away with something new. I am not the main benefactor of this training. The citizens of Greenville, Texas and Hunt County, Texas, as well as the north Texas area reap the benefits of this training with better recovery rates for property as well as more perpetrators being taken off the streets. NCFI also trains prosecutors and judges in protocols and also in evidence.

Mr. RATCLIFFE. Thank you, Detective Waddle.

I will now recognize myself for an initial round of questions for our distinguished panel.

Let me start with you, Mr. Davis. As you know, prior to being elected to Congress, I served on the Advisory Board at TEEX, and so I am very familiar with your organization. It is the largest homeland security training facility in the world, I think some 200,000 folks a year.

Mr. DAVIS. Yes, sir. That is exactly correct.

Mr. RATCLIFFE. So it is just a terrific organization, and again I am thankful that you are here today.

So in your capacity there at TEEX, I would be interested in your perspective on what are the key challenges with cybersecurity training at the local level going forward.

Mr. DAVIS. Yes, sir. Thank you. First of all, to your comments regarding TEEX, because we are serving and extension is part of our mission, I would think that my perspective is the awareness issue that training is available that is DHS/FEMA-funded training, sir. I reeled off some numbers of 32,000 that we have trained across the United States, but when we look at what portion of those numbers come from the State of Texas, for example, or if I go to State and local districts, those numbers are very, very small.

So I think the issue is the awareness in accessing that training that is available. One of my fellow panel members mentioned the need for training, and of course I passed my cards out here. But we go to those jurisdictions so they don't have to spend any money sending them to us. We do direct-delivery, face-to-face training.

So the short answer to your question is awareness and accessing—not access, but accessing——

Mr. RATCLIFFE. So as a follow-up, do you know that even here in this audience there are a whole bunch of local community representatives that could be the beneficiaries of that type of cyber training TEEX offers? So how can they get it?

Mr. DAVIS. Yes, sir. We have on-line training at www.teex.org. If you go on our website you will see a section on cybersecurity training, and anyone that is in this audience can, in fact, access that training on-line.

Mr. RATCLIFFE. So, a follow-up question. Is TEEX right now in a position to—or how is TEEX leveraging any relationships or partnerships with the Department of Homeland Security at the National level?

Mr. DAVIS. Yes, sir, we are. I had some details in my statement. But first of all, we think it is always important to address any issue as a team. I think you used the team sport analogy there. There has recently been a reorganization of several entities at the DHS level to become more operationalized, okay?

There is a young lady here with me today, Ms. Rebecca Tate. When we started doing cyber training back in 2010, we visited first with our program manager—back then it was also called NCSD, National Cybersecurity Division—and the Infrastructure Protection Directorate. We went to them to talk about those things we were hearing from State and locals.

So we met with them on a regular basis to actually find out what training needs did they see at the National level, and I am proud to say we are on our third course now that is a result of that collaboration. We did a recent course in the States of Utah and Rhode Island that brings cyber and infrastructure protection together, and that is a direct result of our collaboration with those folks in DHS.

Mr. RATCLIFFE. Terrific. Thank you.

Chief Greif, let me turn to you. You bring to us today a wealth of professional experience with different public safety organizations. I know you are here today as a spokesman for the IAFC. So

let me ask you, when Congressman Burgess and I and others at the National level talk a lot about the importance and the need for coordination across critical infrastructure sectors to encourage cyber resilience, how are those efforts or how do those efforts impact public safety organizations at the State and local level like you have been involved with?

Mr. GREIF. For example, we have fusion centers that are often funded with Office of Emergency Communications funds. Those fusion centers allow all of the common agencies, the necessary agencies to mitigate any type of emergency situation, to come together with all stakeholders. The more we are coming together and sharing some information with one another, that would be one example of how that benefits us. At the National level, the funding trickles down to the local jurisdictions.

As I said earlier about the Super Bowl, I had no idea until I was put on that committee just what-all goes into a major event like that, the planning with all the different agencies throughout the 4-county region that came together. We met monthly for a year just on my committee, which was communications. A big effort was talking about all the resources that were available to us, protection as well as workarounds, what to do in case of——

Mr. RATCLIFFE. I am glad you mentioned that because as a follow-up and in your testimony you talked about it being worthwhile to study the effects of cyber attacks on public safety organizations. Are you aware of anyone who is putting together sort-of a best practices with respect to public safety organizations and cybersecurity practices?

Mr. GREIF. One of the efforts that is underway is I chair a—I am on the board of directors for a public safety communications agency. The DHS has actually sent members a few times a year when we meet annually, and there is a panel of experts. It is made up of IT personnel, information technology people, as well as fire, police, EMS, and they are working on a document just like that, that came out at last year's meeting.

So certainly it is on the forefront of our consciousness. We are doing everything we can to piggyback on Mr. Davis' comments. It is knowing, understanding what is out there. There is some wonderful training available. It is getting personnel to understand that the fire and police, especially speaking for my brethren, that we understand the necessity for us to get involved in the critical questions we need to be asking.

Mr. RATCLIFFE. Terrific. I noticed in your testimony you talked about segregating the CAT and the 9–1–1 systems for security purposes. Is that common?

Mr. GREIF. I can't say for sure because I have only been a part of two jurisdictions, so I don't want to get too specific, but I don't believe that it is widely spread. We were very cautious where I came from. We wanted to make sure we took all reasonable means, even though that added some complexities to day-to-day life. The more you secure something, the harder it is sometimes to operate it or update it. But we felt it was worth the trouble to keep it segregated.

Mr. RATCLIFFE. Terrific. Thank you.

I do have some additional questions, but I want to yield to Congressman Burgess. As I mentioned, I am very grateful that he is here today at this subcommittee hearing. He represents the 26th Congressional District of Texas, which sounds like it is a long way away from the 4th District, but it is really next door. He represents all of Denton County and most of Tarrant County as well. He serves on the House Energy and Commerce Committee, and in that capacity he also is the Chairman of the Subcommittee on Commerce, Manufacturing, and Trade, and he is very steeped in cybersecurity issues. In that role he has been a leading voice in Congress on the data breach issues as cyber criminals focus on more fraudulent activity that affects more Americans and that affects commerce. He has been a leading voice with respect to the need for legislation in that area.

So with that, I want to recognize Congressman Burgess and yield him as much time as he may consume to provide some remarks on the issue of data breach questions he may have for our panel.

Mr. BURGESS. Great. Thank you, Chairman.

Thank you all for being here. Thank you for allowing me to be here.

Chairman, it is not lost on me that this is a field hearing, and I am sure your district is grateful that you are doing it and you are here on the campus. Even though we are not in the Rayburn Room, Mr. Rayburn, this is his district. So it is fitting that we are here.

I do serve as the Chairman of the Subcommittee on Commerce, Manufacturing, and Trade. We are concerned about data breach episodes that have occurred and the consequent notification that is or should be required for the protection of the consumer when these breaches do occur. So while Chairman Ratcliffe is Chairman of the subcommittee that deals with the .gov side of the world, we deal with the .com side of the world. But as I tell people all the time, it doesn't really matter. Data security is National security, and if you forget that fact, then you are going to be upset at some point, which we all found last year at tax filing time and we rather expect it may come up again in a couple of weeks when the income taxes are filed and people realize that they can no longer file their taxes on-line because their accounts have been diverted in the past and monies have gone inappropriately.

The good news is the taxpayer is eventually made whole. It does take longer for them to get their refund. The bad news is that the Federal Government actually is refunding that money twice. It is unlikely they will recover it for the individual who is inappropriately reimbursed, and this is no surprise because of the behavior of someone who would do that. Sometimes they over-estimate the amount of money they are doing that reimbursement. So it is kind of like a double-whammy for the IRS. I know we got a ton of calls on that last April 15.

Mr. Wilson, I rather suspect that—a lot of our calls started to come from some of our local police agencies when our neighbors called the police department and said, oh my gosh, our taxes have been hacked and I have been robbed. They said, well, let's call your Congressman and he will fix it.

[Laughter.]

Mr. BURGESS. True, but it took some time, and it was very uncomfortable all around.

I really got interested in the data breach notification. All of us are consumers, and we hear the big stories about the big breaches, and then the data is taken. It is data that is at risk somewhere and you don't really know what anyone is doing with it. But from the consumer's perspective, when do we need to be notified? It almost seems like we have breach fatigue because we hear so much about breaches. I am not going to worry about it anymore because I just can't worry about all of these things that I am hearing.

So we really did try to set the parameters around a National data security standard and for when that breach notification threshold should be triggered, and if law enforcement says we need more time, that they be given more time. But if law enforcement's time frame is okay, then the person who was holding the data that has subsequently been breached, that they have a certain time frame in which they must notify the individual. Right now, the bill has passed through the subcommittee, our subcommittee and our full committee, and it is awaiting floor activity right now. That time frame is set at 30 days.

In setting a National security standard, it is your duty to tread carefully because there are 51 State jurisdictions, if you include the District of Columbia, more if you include the territories, who may already have their own ideas about what these data security standards are, and I am sensitive to that. The Commerce Clause is sometimes over-used and over-interpreted by the Federal Government.

But this is one of those times when I try to envision the Founding Fathers sitting down and writing those Article I conventions: What are the powers of the Congress? The regulation of interstate commerce, the trade between the Indian tribes—well, okay, they were 100 years before the telegraph, 150 years before the telephone, 250 years before the internet, but they were probably thinking of e-commerce when they wrote the Commerce Clause into the Constitution because e-commerce, by definition, needs to flow seamlessly across the borders of those States, and the Commerce Clause was absolutely necessary for e-commerce to exist. We want to be sensitive to that.

To the extent that a National standard is set, States do need to have a big say in what that floor is that is going to be established, and the State attorneys general. The provision that passed through the committee, the full committee, was that the Federal Trade Commission would use existing enforcement authority. We did not want to create a new enforcement authority because we already have enough Federal agencies. But the Federal Trade Commission, using its existing authority on deceptive and unfair trade practices, would exercise that authority. But the attorneys general of the several States would be able to bring their own cases under those FTC provisions if the FTC was not moving fast enough, which will occur from time to time.

That bill has passed through the subcommittee. It is awaiting floor activity.

I wake up every morning kind-of living in fear of, when is the next shoe going to drop on this? You hear about a big company,

and they have been hacked, and they took all these records, and they are sitting somewhere, and nothing is really happening with that. When is the other shoe going to drop on all of those people who were exposed in that breach?

The other thing that we really have just begun to scratch the surface of in our subcommittee, and I know Chairman Ratcliffe will work on it in his subcommittee, is it is terribly frightening to me as a physician to think about the denial-of-service activity that has been hitting some health care organizations. To think of having a fragile medical patient in the ICU, and you walk in in the morning and you say may I see the chart of the overnight vital signs of my patient, and they say I am sorry, sir, it has been encrypted, and we don't have the key. I mean, what a dreadful situation to find oneself in.

Mr. Wilson, I think you mentioned it in your testimony, about coming up with, how do you set the deterrence on some of these activities?

Mr. Chairman, I would just say I think in the case of ransomware applied to a health care organization, the deterrence ought to be, "You will be shot at sunrise," and perhaps that will do it, because this is a life-or-death situation with these patients where their medical records have been encrypted by a criminal.

But again, very useful panel for me. We do an emergency preparedness summit in my district usually in April of every year. I will be doing one in a couple of weeks. We live here in an area where severe weather can happen in the month of April. It can happen any month, as we learned this year, but April is when we are most at risk for that. So I am very interested in some of the things I learned this morning about—you protect your systems. You conflate a denial-of-service activity with a Super Bowl, and that is a big deal. You know the criminal mind is just ever—things spring from it all the time, and you just can't help but wonder what criminals might be thinking about.

But let me just start with you, Mr. Davis, and your training. You mentioned you have some on-line instruction courses——

Mr. DAVIS. Yes, sir.

Mr. BURGESS [continuing]. That are available?

Mr. DAVIS. Yes, sir.

Mr. BURGESS. Would you tell me just a little bit more about this? Can average citizens access those, or is that something that is perhaps reserved for the chiefs personnel in part of their professional training?

Mr. DAVIS. The average citizen, Congressman, can access those, and it is good basic information. I will give a personal example, and I hope my wife doesn't get to see this——

Mr. BURGESS. It is just between us.

Mr. DAVIS. Just between us boys here, right? Okay.

I got an email from a friend that said, hey, be careful. This is a colleague at work, and I forwarded it to my wife. As I was forwarding it, she was calling me or texting me to tell me that, hey, I just got some information, re-verify my account number, my password, my this, that, and the other. She was doing a couple, 3 things. These shows that come on at 11 o'clock, these people, okay?

She had given them all her information. I said, my gosh, did you read the email I sent? She didn't.

So when we talk about those things, when we talk about the on-line courses, the general users, which talks about really those things you need to be aware of, okay? Even now, even I am more sensitized. Even when I get busy and I am looking at an email, if I don't recognize somebody, I get more emails from auctioneers, go pick up your money at the bank, we need your account because we want to deposit something, and I go delete, delete, delete.

So to answer your question, sir, they are available on-line at *www.teex.org,* and the average citizen can access those courses, and I recommend that they take them.

Also, last, let me say there are 3 States right now, Arkansas, Louisiana, and Wyoming, and also a college, Fresno Pacific University, where they are requiring their workers to take our on-line courses.

Mr. BURGESS. So part of my question, then, is do you provide some credential for the person who has satisfactorily completed the——

Mr. DAVIS. Yes, sir. They get a certificate for completing an on-line course, and I think more importantly than the certificate, they gain some knowledge that they can spread around geometrically about how to protect their own information.

Mr. BURGESS. Seems like it would be a useful thing for a homeowner's insurance policy. You know, sometimes we will give a break to someone who takes a defensive driving course.

Mr. DAVIS. Yes, sir.

Mr. BURGESS. On their automobile insurance. This might be one of those places where the insurance company might want to be proactive, and I am glad that you are providing the service.

Mr. DAVIS. Yes, sir.

Mr. BURGESS. Is there a charge?

Mr. DAVIS. There is no charge, sir, but I think you have just given us an idea to really reach out to insurance companies and say, hey, here is an idea here, because you are right, I have done that to get that discount. Dad doesn't teach me to drive. I pay somebody——

Mr. BURGESS. Very wise.

Chief, let me just ask you, in your previous role when you were at the City of Fort Worth—of course, I don't want to get parochial here. Forgive me, Chairman, but we have a Super Bowl twice a year in Fort Worth called the Texas Motor Speedway, and that will be happening this month. The Commander 500 I think is the name of the race. Do you have as many people come to the Texas Motor Speedway as come to a Super Bowl?

Mr. GREIF. Yes.

Mr. BURGESS. So even though the Super Bowl is unique, you have these large, widely-attended events that happen in the city of Fort Worth. I assume there has been kind of a learning curve with that, but it gets back to the question that Chairman Ratcliffe asked. How do you share that best practices information from managing those large, widely-attended events with other jurisdictions?

Mr. GREIF. I am certain it is still going on. I am actually glad I won't have to be part of that planning committee. We used to

tease the Arlington folks about we do Super Bowls twice a year, as you alluded to. It starts months in advance, holding meetings. You hold these meetings so often, you start building personal relationships where you get to know Captain Webster from Texas Department of Public Safety. I met more people throughout the Denton region.

We came together and started about 3 or 4 months in advance of each race, and you just literally shared as much information as possible across lines with one another. As I said, it is so important to prepare for a cyber attack and prevent it, and you have to have preparations, which I won't go into details about, but what do you do when one actually occurs? You need to have back-up.

Those types of meetings are a mini-fusion center when it really comes together and we sit there and spitball and come up with ways to mitigate. So it is just a series of meetings, sir.

Mr. BURGESS. Let me just ask you a question. We do have some students in the audience, and you referenced the UASI program. The former mayor of Mont Creek taught me a number of new words, and UASI was one of them. I thought it was a pejorative term when he first used it because when those initial grants came out, if I recall correctly, as the Department of Homeland Security was being organized, the UASI grants were administered regionally. They were delivered to Dallas and expected to be shared with Fort Worth, and I just remember the mayor having some issues with that.

But for the students here, could you kind-of go through what the UASI program is?

Mr. GREIF. Well, a Federal program that provides funding for fire and police in other jurisdictions as well, but obviously those are the ones I am most concerned about, and many things get funded out of that, like training opportunities. We can hold anything from hazardous materials classes, where that funding not only was paying for our personnel to go get the needed training, but it was paying for the backfield because you still had to have troops driving trucks to keep the city safe, to hardened equipment. It is amazing.

Again, some of the stuff is somewhat—I won't talk about necessarily some of the equipment that was purchased to protect the community, but a major expense in equipment was purchased for the protection of many different types of terroristic activities, and that equipment was in place in cities all across central Texas because of UASI.

Mr. BURGESS. Chairman, I will yield back to you, and if possible I will do a second round as well.

Mr. RATCLIFFE. Perfect. I thank the gentleman.

Detective Wilson, I want to take advantage of the fact that you are here on behalf of the Dallas Police Department, obviously one of the largest, most visible police departments in the United States. I am just curious if you can offer perspective on what the daily cyber threat looks like at the Dallas Police Department.

You talked about in your testimony reliance on computer networks for operational and for investigative functions, so I assume that you have to take that into account in terms of the daily threats that are coming into the Dallas Police Department, and

also take that into account in how you are training your personnel to deal with those threats.

Mr. WILSON. Well, as you said, the Dallas Police Department is the ninth-largest police department in the country, the second largest in the State. So we act as a nexus for a lot of information sharing, as well as collection. Daily, we get notifications from agencies asking for information to support an investigation or some type of threat that they have uncovered, to give them the guidance or put them in the right direction, who is the expert who can go in and help them.

Unfortunately, the Dallas center does not have a technical expert within the center that deals with cybersecurity, but as part of the approach to dealing with a wide varieties of crimes that we deal with, we have a partnership with our Federal agencies, and we have an expert within the Dallas Police Department who actually works with a task force and the FBI. We also have a couple of officers that deal with computers, and they have been doing it for years and years. We find that as they continue to perform these functions and people know the capabilities that we have, we are increasingly tasked with trying to assist other agencies.

As a fusion center director, I see most of the emails that come into our center on a daily basis, so my email averages approximately 200 to 300 per day coming in from Federal partners, State partners, local partners, and from other States as well, trying to reach out to you, to take advantage of the network.

As we look forward to increasing our ability to address the cyber threats, we basically have 2 problems. One is stop the cyber threat in itself, and No. 2 is how do you pursue the cyber threat actor, the person who actually committed it, and to what extent do we go to prosecute? That definitely leans toward our Federal partners. That is their jurisdictional area. They have the resources and the expertise oftentimes that we do not have, and they are always looking to try to assist us in these types of situations.

Mr. RATCLIFFE. Terrific. Thank you, Lieutenant.

Detective, I actually had a bunch of questions for you, but your testimony was so thorough that you pretty much covered it. I wanted to ask you about your experience with the Electronic Crimes Task Force and, of course, the NCFI, National Computer Forensics Institute, which my bill would authorize into law. I really appreciated your testimony. You spoke eloquently of how it benefitted you with respect to your career, but also benefitted the folks that you serve as a detective in Greenville. I just think that, more than anything else, it is a great message, and I hope that as you go into retirement that you will still continue to be a great ambassador because I think that is what you are, an ambassador for how State, local, and Federal partnerships, particularly as they pertain to National security issues and cybersecurity as a National security issue, how they are supposed to work.

We all know that 9/11 was a communication failure in many respects, and we have worked hard in trying to eliminate that, and with respect to the threats in cyber space and cybersecurity, we want to avoid a cyber 9/11, if you will. So some of the programs that you have been a part of, some of the partnerships that you

have been a part of have prevented that up to this point in time and, I think, can in the future.

So again, I just appreciate you being here today, your testimony, and what you stand for in that respect.

I am just going to close with a question for anyone that wants to take it, or all of you that want to take it. We asked the question about what are the key challenges, and from your testimony many of you talked about the financial side of things and, obviously, fundamentally the role that Congressman Burgess and I and others in Washington can play with respect to that and how that affects workforce issues.

But are there authority issues out there that we can help you with in Washington? In other words, are there things from an authority perspective that we should be legislating on in this space that you think need to be addressed? Anyone.

Mr. WILSON. I would say that the proper authority for investigating cyber crimes is the way that you can get the most impact, obviously, achieve a conviction. I would love the Federal system to stay for the day instead of 1 day or 3 days. So oftentimes, when we can't get the impact to take that offender off the streets in a time that we consider to be reasonable, we turn to our Federal partners. They have a much wider reach, a little bit bigger handle to hit them with it. They are most gracious and most times if they can do so, they will. They have expanded powers. I believe that through legislation you will find it will be even a stronger growing trend from a local perspective to turn around and say rather than a State trial, let them go and see what they can do to stop that behavior. That would be my perspective.

Mr. WADDLE. I kind-of go along the same lines. We see so many repeat offenders that go off and that use our State prison systems as education. I think that we have to be stiffer in our punishments with these offenders because of the amount of damage they do monetarily and even physically. So maybe some stiffer enforcement.

Mr. RATCLIFFE. Thank you.

I again recognize my colleague for any additional questions he may have.

Mr. BURGESS. Thank you, Chairman.

Detective, you did an excellent job of detailing how you had received the training and being able to provide protection for the people of your jurisdiction. We live under the tyranny of the Congressional Budget Office where we work, and everything is looked at as a cost. But as I listened to you provide your testimony, it also occurred to me that there was value brought back to your department, to Greenville, value back to the community, and sometimes it is very difficult to dissect out. When we look at something on a sheet of paper, on a spreadsheet, it is just a cost, and we deal with this in health care all the time, and it drives me nuts. But there is really no way to offset the cost with the value that you brought back to your community.

Just as we conclude the hearing today, if there are thoughts that you have on that that you would like to share with us about how to better tease out that value figure, whether there is a fraction or a multiplier that could be applied. Perhaps in your experience you

have encountered either some examples or even a formulaic approach, this much was invested in the activity that I undertook, but this much was delivered back to the community.

Mr. WADDLE. The one thing that I failed to mention in my testimony was that not only do I cover Greenville, but I also assist the local agencies in Hunt County. Privately in our office I did that, but also at the Electronic Crimes Task Force, we covered most of North Texas. So we assisted agencies from Denton, from Steubenville, from Tyler, Lindale, that area, all the way out to Texarkana. So the training that I received has been able to help me help those people.

There is a cost, and I understand that. Again, I don't question that. We had the same problem in the city, the city manager saying, well, you don't need to spend that. I understand that. But when we can benefit, and in my case, with the experience that I have, when we can benefit our own citizens and those around us, and they know that they have somebody that they can contact to get answers, I think that the money spent is spent well because it benefits so many people in getting answers to their questions and assistance in their investigations.

Mr. BURGESS. Intangible, difficult to calculate for a return on investment, but it definitely exists, doesn't it?

Mr. WADDLE. Exactly.

Mr. BURGESS. Thank you, Mr. Chairman. I will yield back.

Mr. RATCLIFFE. I thank the gentleman.

I thank all the witnesses that have been here today for your valuable testimony.

Again, I thank Congressman Burgess for being here and bringing his insights into this important topic.

Other Members of this committee that aren't here today may have some additional questions for our witnesses. So if that happens, we will ask you to respond to those in writing.

Pursuant to Committee Rule 7(e), the hearing record from today will be held open for 10 days for Member statements and for follow-up questions.

In closing, let me just again say thank you to everyone that is here today, that has participated in putting this together, and thanks to everyone in Grayson County for letting me bring the Washington road show here to my home district.

With that, without objection, this subcommittee stands adjourned.

[Whereupon, at 12:22 p.m., the subcommittee was adjourned.]

APPENDIX

QUESTIONS FROM CHAIRMAN JOHN RATCLIFFE FOR ALPHONSE DAVIS

Question 1. Are State and local governments ever the target of nation states, hacktivists, or criminals and are they aware of and taking advantage of the protections that DHS offers through its Enhanced Cybersecurity Services program?

Answer. State and local governments are targets currently under attack with unstructured, structured, and highly-structured attacks. These attacks range from the unstructured "script kiddies" looking for low-hanging fruit to the less-frequent, highly-structured attack from nation states looking to gather information. We are also aware of motivated actors from foreign organized crime organizations utilizing ransomware in our country, even at the local Government level—a trend that seems to be growing.

Our experiences and relationships across the country indicate that the DHS-supported NIST Cybersecurity Framework is gaining recognition and respect within local and State communities, as well as with small, medium, and large businesses. However, widespread awareness and adoption of the DHS Enhanced Cybersecurity Services (ECS) is in the very early stages. ECS needs more exposure in order to educate local and State governments on its availability and capabilities, with additional information on how to request the services.

Question 2a. How does TEEX decide what cyber-related training courses to offer? How are those courses evaluated?

Answer. For the development or continuation of any cyber-related training courses, we conduct a needs analysis to examine gaps in operational knowledge and capabilities, gathering data from National surveys, utilizing publicly-available data on training needs (from reports such as the 2015 National Preparedness Report), and interviewing State and local contacts regarding their needs. As part of that needs analysis, we evaluate the scope and priority of the need, the audience, the method of training delivery, and the availability of duplicate or similar training.

In some instances, the development of a new course is initiated by Federal partners. Most recently, the "Physical and Cyber Security for Critical Infrastructure" course was developed through a collaboration between DHS Cybersecurity and Communications and the DHS Office of Infrastructure Protection. They recognized the need for a better understanding of the interdependency between physical and cybersecurity at the local level as well as the need for communities to collaboratively formulate enterprise risk management strategies, enhancing infrastructure security and resilience efforts. The DHS departments worked with TEEX to develop the course that meets that need.

During the recent revision of a course on "Community Preparedness for Cyber Incidents," we examined the gap identified between Emergency Management and Information Technology. We conducted interviews with people in these disciplines to identify what they need to learn to be better-prepared for the ever-increasing and ever-evolving threat of a significant cyber incident. We are in constant communication with State and local governments, and they often describe what they are seeing in their communities and ask how we can assist.

Question 2b. Are they assessed or updated regularly, due to the changing cyber landscape?

Answer. Our courses undergo a needs analysis and recertification every 3 years in order to remain relevant and current. In addition, our courses are continually evaluated through participant feedback to identify improvements and updates prior to a schedule update.

Our program staff (instructors, curriculum developers, managers) dedicates a significant amount of time each week researching and learning about the latest trends and threats in the cybersecurity landscape. This information is used to update course content and for use as updated examples in course deliveries. We also keep

in close touch with our DHS partners and add information to our courses about new DHS resources and assistance available as we learn it.

QUESTIONS FROM CHAIRMAN JOHN RATCLIFFE FOR SAM GREIF

Question 1a. How important is coordination across critical infrastructure sectors for encouraging cyber resilience?

Question 1b. How do these efforts impact public safety organizations and State and local entities?

Answer. As you can imagine, it is vitally important that critical infrastructure sectors share information about potential threats. Local fire and emergency medical service departments need to be warned of potential cyber threats, so that they can take the appropriate protective action. For example, while there have been well-publicized stories in the media about hospitals having to deal with the effects of ransomware incidents, local fire departments also have had to deal with these problems. In January, the city of Snoqualmie, Washington, paid a ransom of $750 to hackers that took control of a computer at the Duvall Fire District.

I receive notices of possible threats from the local Plano police department, the council of governments, and the Homeland Security Information Network, among other resources. This information, and the lessons learned from cyber attacks, is key to preventing or mitigating these threats. It is important to recognize that the ease of implementing a cyber attack may encourage a lone-wolf terrorist or criminal, who otherwise would not want to risk personal injury in a kinetic assault on a fire or police station. So we may see an increase in these threats in the future. Again, thank you for the opportunity to participate in the discussion on this important topic. The threat of cybersecurity only continues to increase. The Nation's fire and emergency service must be prepared for it.

QUESTIONS FROM CHAIRMAN JOHN RATCLIFFE FOR RICHARD F. WILSON

Question 1. Are State and local governments ever the target of nation states, hacktivists, or criminals and are they aware of and taking advantage of the protections that DHS offers through its Enhanced Cybersecurity Services program?

Answer. The city of Dallas has in the past, and with daily incidents, been subjected to, and been the subject of adversarial attacks by foreign powers, foreign extra-territorial actors, National and local hacktivists, criminals and unclassifiable agents.

The city, in addition to local defensive capabilities, also utilizes the services and cyber-intelligence capabilities provided by Department of Homeland Security, DHS, and other National (private and public) capabilities.

Question 2a. How important is coordination across critical infrastructure sectors for encouraging cyber resilience?

Question 2b. How do these efforts impact public safety organizations and State and local entities?

Answer. It is extremely important and a necessity to have a structured, systemic coordination, incident response collaboration, monitoring, quality capabilities and management between the SLTT and central government.

The impacts these types of activities provide to public safety organizations, and State and local entities are more structured protective strategies, more pro-active incident alerting, and responses that leads to faster incident identification and management. This in turn ensures that outcomes of these incidents are managed effectively and timely, thereby ensuring that the adverse potential outcomes of these incidents, do not overburden the local resources and capabilities.

QUESTIONS FROM CHAIRMAN JOHN RATCLIFFE FOR DON WADDLE

Question 1. How was your work with the Electronic Crimes Task Force (ECTF) valuable to your career as a detective?

Answer. In my police department, while working as a detective, I worked property crimes, which covers theft, criminal mischief, stolen cars, and fraud. Prior to being assigned to the North Texas Electronic Crimes Task Force, there was only a few ways for me to go at fraud. This would be what I read in books or by getting guidance form our prosecutors. After getting on the task force I learned more by being involved in investigations with other agencies and with helping Federal authorities with their investigations. I was able to share my knowledge with other members of law enforcement and was also able to build up my knowledge in investigating fraud. I was also able, because fraud oftentimes involves computers and cell phones, to learn about computer and cell phone forensics. By being assigned to the task force I learned more about the crimes I was investigating, and was able to use that

knowledge to prepare better cases for prosecution, and to bring answers to my victims of crime.

Question 2. How did your work with ECTF differ from or support your work as a detective in Greenville?

Answer. I do not believe my work with the task force differed from my work as a detective in Greenville. My job is to investigate crime and I did that in both places. I built a strong network of other investigators that could help me if I had a question, or I could help if they had a question. When I think of supporting my work as a detective in Greenville, I would probably never have been able to conduct the investigations I conducted without the equipment and training I received as a task force member. One case in particular was a defendant who stated he talked to another person very infrequently, but when I examined both phones I was able to determine that they had numerous conversations all the time. This was done using equipment and training I received while assigned to the task force. I also had Federal partners that could come in and help me with my investigations, and if need be, could assist me in preparing for a Federal prosecution of the case.

I hope that my answers to your questions provide enough information for you to make important decisions related to Cybersecurity, Infrastructure Protection, and Security Technologies.

I want to stress that I am extremely grateful for having been on the North Texas Electronic Crimes Task Force and the training and equipment that I received. The city of Greenville and all of Hunt County, Texas, benefitted from my association with the Electronic Crimes Task Force.