Statement of Subcommittee Chairman John Ratcliffe (R-TX)
Cybersecurity, Infrastructure Protection, and Security Technologies Subcommittee

"Value of DHS' Vulnerability Assessments in Protecting our Nation's Critical Infrastructure"
July 12, 2016

Remarks as Prepared

The Subcommittee meets today to examine how the Department of Homeland Security is fulfilling its important mission of protecting our nation's critical infrastructure. We look forward to examining DHS's capabilities in conducting physical and cybersecurity vulnerability assessments. The critical systems that are central to our daily lives are targeted every day by terrorists, nation states, and criminals. Taxpayer funds used to protect these systems must be invested wisely and must add value for owners and operators. Because threats to critical infrastructure are numerous and diverse, we're interested in learning specifics about the strategy that guides DHS' efforts in this area.

I want to thank our panel of experts for joining us so Congress can better understand the work being done in this area and the value of DHS's vulnerability assessments and training.

For 12 years, the primary mission of the Office of Infrastructure Protection's Protective Security Advisor Program has been the protection of critical infrastructure. Protective Security Advisors (PSAs) are regionally based in alignment with the ten FEMA regions. PSAs execute their primary mission through the planning, coordination and performance of security surveys, assessments and outreach activities to those critical infrastructure owners and operators that elect to participate in these voluntary programs. PSAs also support National Special Security Events, Special Event Activity Rating (SEAR) Level I and II events, and respond to incidents.

The mission I just described is enormous. And because it is voluntary in nature, its success hinges on stakeholder buy-in. Such buy-in requires strategic outreach and real value added for owners and operators of critical infrastructure. I am interested in hearing what strategy is guiding this important program and what metrics DHS is using to track and increase such value.

In 2014, DHS established the Critical Infrastructure Cyber Community Voluntary Program to help organizations address and improve their cybersecurity risk management. Additionally, DHS created the Cybersecurity Advisor Program, or CSA Program, to provide cybersecurity expertise and voluntary cybersecurity programs to critical infrastructure owners and operators. While the CSA Program is still in its infancy compared to the 12-year old PSA Program, the CSA mission of assisting our nation's critical infrastructure owners and operators in strengthening their cyber hygiene is critically important. With the passage of the Cybersecurity Act of 2015 last December, we must ensure the CSA program is also guided by a strategic plan and is well-positioned to effectively lead DHS's cyber engagement efforts for critical infrastructure.

Last month, this Committee unanimously passed the Cybersecurity and Infrastructure Protection Agency Act of 2016 (CIPA) to elevate the functions of our nation's cybersecurity and critical infrastructure

protection into an operational component within DHS. The legislation recognizes the unique expertise required of both the cyber and physical aspects of the Agency's mission while also stressing the importance of enhanced collaboration and coordination between the cyber and physical missions.

The Government Accountability Office has reported extensively on DHS vulnerability assessment programs for critical infrastructure and identified challenges within DHS in 2013, 2014 and 2015. These reports included number of recommendations to increase the use and enhance the participation of stakeholders in these vulnerability assessments.

One particular area of concern found in the report was "federal fatigue," which results from a perceived weariness among the private sector who might be repeatedly approached or required by multiple federal agencies to engage in risk assessments. "Federal fatigue" is particularly alarming, as the PSA and CSA assessment programs at DHS depend entirely on voluntary participation.

Just last week, a review of the DHS's website for critical infrastructure vulnerability assessments found conflicting and outdated information. While errors like these appear insignificant, it's important to remember that these programs are voluntary, and if DHS can't handle basic promotion and marketing of the programs, I have concerns about the likelihood of private sector participation.

The Subcommittee believes both the CSA and PSA programs can be of great value for the protection of our nation's critical infrastructure; but a clear strategy, effective stakeholder outreach, and metrics of success are essential.

It is the hope of the Subcommittee that this hearing will clarify how DHS is working to address these issues. Further, given the relative infancy of the CSA program, the Subcommittee hopes to learn more about CS&C's plan to expand this program and would hope that lessons learned from the PSA Program are being incorporated. This Subcommittee is responsible not only for the oversight of DHS's functions but also for ensuring that it has the tools and necessary authorities to successfully meet its objectives. In that spirit, we welcome input as to how we can assist in this critical mission.

###