Response to Written Questions Submitted by Hon.
Roger Wicker
Written Questions for the Record to
The Honorable Michael Chertoff

Question 1. What is your experience with the WHOIS database from a cybersecurity perspective and can you comment on its importance in this regard?

An unexpected side-effect of Europe's adoption of the General Data Protection Regulation (GDPR) was the decision of the Internet Corporation for Assigned Names and Numbers (ICANN) to redact some registration information from its WHOIS database. ICANN is the non-profit organization that manages the global domain name system, which acts as a sort of address book or telephone book for the internet, directing users to specific servers based on the domain name information that they enter into their browser. This allows end users to type in the domain www.whitehouse.gov rather than having to memorize the specific server address associated with the White House's public website, which could be a series of up to 32 alpha-numeric characters. ICANN's WHOIS database allows for the pubic, and security researchers, to look up key information about individual domains, including who registered or controls them.

ICANN has interpreted GDPR as requiring the redaction of several fields of data traditionally included in WHOIS data, including the name of the person who registered the domain, their phone number, physical address, and email address. While this information is not always publicly available through WHOIS (and can be of dubious quality) as a result of varying practices from various domain name providers, this data can be very useful to researchers, criminal investigators, and other parties seeking to investigate potential cybercrimes or malicious activity associated with a specific domain (which may, for example, be used to mimic a major retailer in order to steal user credentials or serve as a command and control server for malicious software). As a result of this change, ICANN has proposed creating an "accreditation" system to restore access to this information to law enforcement and researchers. It has yet to fully develop such a system and has indicated that it would be ready until at least December 2018. It would then likely take several months for domain providers to adopt the new system.

As a result, for at least the next few months, researchers and law enforcement will be unable to utilize a tool that has historically been useful in shutting down cyber criminal enterprises and in the conduct of cyber criminal investigations. I would encourage ICANN to move quickly to remedy the problem and restore access to this information to both law enforcement and researchers in order to help them combat cyber criminal activity.