Scot F. Rogers
EVP & General Counsel
F5 Networks, Inc.

Testimony before the Senate Committee on Energy and Natural Resources
Field Hearing on Oversight of the Department of Energy's Functions and Capabilities to respond to Energy Related Emergencies, Including Impacts to Critical Energy Infrastructure

Thank you Senator and Mr. Secretary for giving me an opportunity to provide information to this Committee and be a part of this panel to discuss topics we at F5 believe are of critical importance to the safety of our country.

I would first like to give you a little background on my employer, F5 Networks, a worldwide leading developer and provider of software-defined application services. We are based here in Seattle with over 4,300 employees in offices around the world. Applications have become the gateway to critical and sensitive data and our mission is to help organizations deliver the most secure, fast, and reliable applications to anyone, anywhere, at any time. Our offerings include software products for network and application security, access management and a number of other network and application services. We also offer distributed denial-of-service **(**DDoS) protection, application security and other application services on our cloud-based platform. In conjunction with our customers and partners across a variety of fields and industries, we are closely watching the evolution of the cyber-threat landscape for organizations in the 21st century.

Disruptive technology trends are dynamically altering the threat landscape for organizations operating in today's world. The explosion of new software applications, the emergence of cloud computing and the internet of things (IoT) combined with an increasingly mobile work force are leading to the dissolution of the traditional security perimeter. Legacy security architectures are no longer adequate to protect against the evolving threats posed by cyber criminals, hacktivists and state sponsored espionage and sabotage. To borrow from a commonly used analogy, traditional security architectures were akin to building a castle and a moat to secure the king. This castle architecture relies upon utilizing traditional network firewalls and other devices on the network perimeter to monitor and block suspicious traffic on the boundary of the network. In today's world, envision the software application and data associated with that application as a very mobile president who needs the protection of his secret service body guards as he travels the world. As the network perimeter—or in this analogy the castle walls--become more and more irrelevant, industries need to focus on protecting the software applications which front-end their critical and sensitive data, that drive their business and manage their infrastructure as well as verifying the identities of those users who are accessing those applications. The leading technology industry research firm Gartner estimates that 90% of security investment is targeted at securing the network but only 28% of the attacks are focused here. Conversely, only 10% of security investment is focused on securing the software application while 72% of attacks are from application vulnerabilities and stolen user credentials.

Our U.S. energy sector is not immune from these types of evolving threats. In particular, the Internet of Things (IoT) with the inclusion of new smart meters, home power generation devices with connections back into the power grid, and the various interfaces of the Supervisory Control and Data Acquisition networks that control the grid (SCADA networks) create a unique set of challenges. All of these new smart devices are run by new and innovative software applications whose access needs to managed and whose data need to be protected. And where will these emerging energy software applications be developed and reside as the world evolves to a cloud centric model?

All of these unsecured new devices create new threat vectors of attack that must be mitigated. In the world of our energy infrastructure, it isn't the theft of data that is the biggest threat, but disruption to the service or destruction of its means of delivery. On December 23rd of last year, hackers disabled portions of Ukraine's power grid leaving over 200,000 residents without power for several hours. In the attack on Ukraine's power grid, the hackers used compromised user credentials for workers logging remotely into the SCADA network that controlled the grid. In this instance, remote workers weren't required to use two-factor authentication for remote login, which allowed the attackers to hijack their credentials and gain crucial access to systems that controlled the breakers for the system.

The Dept. of Energy has taken steps to help secure our nation's energy infrastructure with the issuance of its *Energy Sector Cybersecurity Framework Implementation Guidance* containing recommendations for implementation of the National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* (NIST, 2014). In the ever evolving world of technology, it is important that organizations stay vigilant to address the exponential threats presented by new technologies and to avoid complacency. A strong focus on protecting not just the networks interconnected to our infrastructure but the software applications that operate and support that infrastructure as well as the users accessing those software applications is critical to the safety and security of our nation's energy sector. Through utilization of web application firewalls, multi-factor authentication and identity federation for secure remote access with consistent, policy based access controls and security data analytics on user behavior, the energy sector can continue to evolve its security architecture to address the dissolution of the network perimeter.

I just want to acknowledge the Committee for recognizing the threats to our energy infrastructure and note that collaboration and unity of effort amongst stakeholders will be critical to meeting this challenge. I would also like to recognize the others on this panel who are here working together to address these issues. Thank you to the Committee for convening this hearing on such timely issues. F5 would also be happy to provide any supplemental materials upon request following the hearing.