Opening Statement of Ranking Member Cedric L. Richmond

Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies

"DHS' Efforts to Secure .Gov"

June 24, 2015

Thank you, Mr. Chairman for convening this hearing on DHS responsibilities in helping all of the federal agencies secure their cyber networks and databases. I want to welcome our witnesses, Dr. Oxment, Mr. Wilshusen, and Dr. Gerstein. Thank you for taking the time to appear before us today.

Securing the federal government's networks and databases is a monumental task. DHS has been charged with the primary task to coordinate and provide cybersecurity guidance for the many federal agencies, critical infrastructure sectors and government programs, whether it be government personnel information, classified background information, patents, taxpayer data, nuclear facilities, health records, port complexes, or any number of other vital government services.

However, under the Federal Information Security Modernization Act of 2014, or FISMA, the White House Office of Management and Budget is responsible for federal information security oversight and policy issuance. However, OMB executes its responsibilities in close coordination with its Federal cybersecurity partners, including the Department of Homeland Security and the Department of Commerce's National Institute of Standards and Technology (NIST).

Both state and non-state actors are attempting to breach our government and commercial systems. And, as President Obama said a few days ago, this problem is not going to go away. It's going to accelerate.

I think we all recognize that certifying the security of information on the Federal government's networks and systems should remain a core focus of the Administration, as we here in Congress should continue to be looking innovative solutions that provide DHS with the authorities to respond quickly to new challenges as they arise.

And Congress must continue our search for legislative initiatives that will help further protect our nation's critical networks and systems.

As a result of the latest government network breaches, we've been told that OMB has launched a 30-day "*Cybersecurity Sprint*" review and recommendations effort. The review team is made up of OMB, the White House E-Gov Cyber and National Security Unit, the National Security Council Cybersecurity Directorate, and the Department of Homeland Security and Department of Defense, among other agencies.

As part of the effort, OMB has instructed Federal agencies to immediately take a number of steps to protect Federal information and assets and improve the resilience of Federal networks.

Specifically, Federal agencies must: immediately deploy indicators provided by DHS, which can identify priority threat-actor techniques and tactics, and procedures and tools to scan systems and check logs, patch critical vulnerabilities without delay and report to OMB and DHS on progress and challenges within 30 days, tighten policies and practices for privileged users, dramatically accelerate implementation of multi-factor authentication, especially for privileged users.

While I'm pleased to see the White House taking immediate action, all of the above efforts are generally recognized as security measures that should already be in place, especially in vital government networks.

I hope to hear today from our witnesses a clear explanation of why many of the standard, recognized security practices were not in place in federal agencies, and clearly identify the plan that DHS has to make sure and certify that federal agencies cybersecurity standards are up to date.

Of particular interest to me in my district, and I know to others on this Subcommittee, is the status of port cybersecurity.

Overall, U.S. maritime ports handle more than $1.3 trillion in cargo annually. The operations of these ports are supported by information and communication systems that, like all other networked systems, are susceptible to cyber-related threats.

Failures in these systems could degrade or interrupt operations at ports, including the flow of commerce. Federal agencies-—in particular DHS—-and industry stakeholders have specific roles in protecting maritime facilities and ports from physical and cyber threats.

GAO did an audit last year of maritime port cybersecurity efforts to assess actions taken by DHS and two of its front-line component agencies, the U.S. Coast Guard and FEMA, as well as other federal agencies.

The GAO found that while the Coast Guard initiated a number of activities and coordinating strategies to improve physical security in specific ports, it has not conducted a risk assessment that fully addresses cyber-related threats, vulnerabilities, and consequences.

The report also noted that FEMA identified enhancing cybersecurity capabilities as a funding priority for the first time in fiscal year 2013.

The study found that FEMA has provided guidance for port related cybersecurity proposals, however, the agency did not include sufficient cybersecurity experts to make sure the multi-level review of grant proposals were thoroughly considered—partly because FEMA had downsized the expert panel that reviews grants.

I look forward to today's testimony on both these issues. It will be crucial that stakeholders appropriately plan and allocate resources to protect ports and other maritime facilities from increasingly persistent and pervasive cyber intrusions.