NSTAC Advancing Resiliency and Fostering Innovation in the ICT Ecosystem Subcommittee Update

November 2018 NSTAC Meeting ● November 14, 2018

Overview

In August 2018, the Executive Office of the President tasked the President's National Security Telecommunications Advisory Committee (NSTAC) to examine the information and communication technology (ICT) ecosystem with three primary objectives. First, identify what technology capabilities within the information and communications technology (ICT) ecosystem are critical to U.S. national security and emergency preparedness (NS/EP) functions. Second, establish where the U.S. has dependencies on those capabilities and if there are market limitations associated with them. Third, review how the Government is managing the risks associated with those dependencies and determine where support for innovation may and consider how to support innovation to help fulfill its assurance needs where there are current or anticipated gaps in capabilities.

The NSTAC established the Advancing Resiliency and Fostering Innovation in the ICT Ecosystem Subcommittee to oversee the report's development. The subcommittee is chaired by Mr. David DeWalt, chairman and chief executive officer of NightDragon Security, and is comprised of 17 individuals from industry and Government who collectively represent a broad cross-section of the information technology, telecommunications, and cybersecurity ecosystems.

Since its launch on September 27, 2018, the subcommittee has held twice-weekly meetings, and begun receiving briefings from external subject matter experts in order to better understand and develop a strategy for addressing the study's core issues. The purpose of this initial research phase is to: (1) identify what technologies and components of the ICT Ecosystem the U.S. depends on for its NS/EP activities; and (2) determine what factors create risk for those technologies, including but not limited to, risk of compromise through cyber means.

At the end of the study's first phase, the subcommittee will produce a letter outlining the above issues, which the subcommittee intends to finalize in January 2019. During the second phase of the study, the subcommittee will develop a full report with recommendations for addressing and mitigating the most critical vulnerabilities to NS/EP infrastructure. The NSTAC intends to finalize this report by March 2019.

Next Steps

At the November 2018 NSTAC Meeting, Mr. DeWalt will provide a progress report to NSTAC members and U.S. Government representatives. He will then discuss the subcommittee's planned next steps for the study and address several parallel U.S. Government efforts relating to supply chain security. Informed by this discussion, the subcommittee will continue its work developing a plan to address critical vulnerabilities to the Nation's NS/EP infrastructure through increased resiliency and innovation in the ICT ecosystem.