OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

AUG 03 2016

MEMORANDUM FOR DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY
COMMANDER, ARMY TEST AND EVALUATION COMMAND
COMMANDER, OPERATIONAL TEST AND EVALUATION FORCE
DIRECTOR, MARINE CORPS OPERATIONAL TEST AND EVALUATION ACTIVITY
COMMANDER, AIR FORCE OPERATIONAL TEST AND EVALUATION CENTER
COMMANDER, JOINT INTEROPERABILITY TEST COMMAND

SUBJECT: Cybersecurity Testing of Systems Hosted in Defense Information Systems Agency Defense Enterprise Computing Centers

Operational test plans provided for my approval often place unrealistic restrictions on Red Teams when it comes to exploiting systems hosted in the Defense Information Systems Agency (DISA) Defense Enterprise Computing Centers (DECCs).

The purpose of cybersecurity operational testing is to enhance security by discovering weaknesses in our systems before our adversaries do. Cyber-threats are intelligent, freethinking actors who do not limit their activities to pre-defined internet locations, pre-scripted tools, techniques, or procedures. Weak interconnected systems are viable intrusion vectors that our adversaries will try to exploit to then move laterally to exploit the targeted system. As such, I expect cybersecurity tests to be comprehensive and operationally realistic to identify problems characterizing the operational risk to the system under test, including attacks via interconnected systems within the DECC.

Restrictions placed on our Red Teams limit our ability to discover weaknesses and offer access paths to compromise and attack by our adversaries. Limiting the Red Team's access to the DECC-hosted system through a pre-defined set of outward facing internet protocol addresses corresponding to the system under test does not adequately characterize the system vulnerabilities and does not support the evaluation of operational mission risks.

In the future, I expect the operational test agencies and DISA to support the Red Teams in their efforts to exploit the system under test from other DECC-hosted interconnected systems, consistent with the validated threat, and commensurate with prudent measures not to damage or destroy data, physically harm the interconnected system, or disrupt critical operations.

J. M. Gil

J. Michael Gilmore
Director