



DEPARTMENT OF DEFENSE
UNITED STATES CYBER COMMAND
9800 SAVAGE ROAD, SUITE 6171
FORT GEORGE G. MEADE, MARYLAND 20755

13 January 2017

The Honorable Joni Ernst
111 Russell Senate Office Building
Washington DC 20510-0100

Dear Senator Ernst,

Let me begin with my personal thanks and appreciation for all that you continue to do in support of the men and women of all our Armed Forces; active-duty and reserve forces, their families, as well as our extraordinary civilian workforce. Your efforts and those of the other members of Congress and the Senate Armed Services Committee, make it possible for U.S. Cyber Command (USCYBERCOM) to successfully execute full-spectrum cyberspace operations.

Like you, I remain committed to providing the most advanced cyber capabilities possible in defense of our nation against an ever-increasing set of rapidly evolving and formidable adversaries. I welcome your assistance in improving our ability to leverage and incorporate the depth of expertise available within our National Guard and Reserve cyber forces.

In response to your question from the hearing on 13 September and most recently on 5 January, there are a number of personnel tracking mechanisms in use by the DoD and National Guard that provide insight into the status of units and capabilities.

The 2007 National Defense Authorization Act, Section 1406, directed, "The Secretary of Defense shall maintain a database of emergency response capabilities," and the 6 September 2016 GAO Report 16-574, "*Defense Civil Support DoD Needs to Identify National Guard Cyber Capabilities and Address Challenges in Its Exercises*" you referenced in your question, recommended that "DoD maintain a database that identifies National Guard cyber capabilities." DoD responded to the GAO report that "Currently National Guard units that are assigned and perform Title 10, U.S. Code, mission report readiness through the Defense Readiness Reporting System (DRRS). Units that are assigned to perform Title 32, U.S. Code mission report to their respective State's Adjutant General."

In compliance with the 2007 NDAA requirement, DoD built a module in DRRS that tracks emergency response capabilities; however, the module does not include cyber capabilities across the National Guard. As this is beyond my area of responsibility, I refer you to Maj Gen James C. Witham, National Guard Bureau who can be reached at (571) 256-7376. For cyber policy within the department, I refer you to the Principal Deputy for Cyber Policy Kate Charlet who can be reached at (571) 256-8016.

Today, under my U.S. Code Title 10 authorities and responsibilities, I track the status and readiness of 133 Cyber Mission Force teams under my command. Of the 133 teams, three are National Guard activated under Title 10 federal mission support. We use DoD's standard Defense

Readiness Reporting System (DRRS) to track readiness of our offensive and defensive teams.

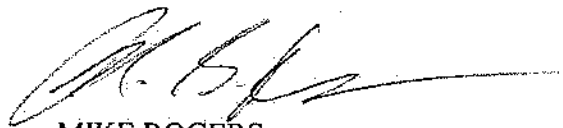
The National Guard is in the midst of unprecedented growth in cyber capacity. The Department of the Army alone is building 21 Reserve Component teams, 11 of which are Army National Guard Cyber Protection Teams (CPT). As National Guard cyber units reach Full Operational Capability (FOC), these units will report readiness through their parent service, similar to any other military capability. The Army and Air National Guard report capability and readiness to the Department of the Army and Headquarters Air Force, via DRRS respectively, and the services report Total Force Readiness to the Department via the Joint Staff. These include Army and Air National Guard cyber units that are activated under Title 10 and gained by USCYBERCOM as Cyber Protection Teams (CPT) and potentially as National Mission Teams to the Cyber National Mission Force (CNMF). The Air National Guard provides two CPT's and one NMT continuously to the CNMF on a rotational basis.

For National Guard response capabilities that are domestic only (Title 32 or state active-duty status and retained by the governor), the National Guard provides a Quarterly Readiness Report to Congress (QRRC). For National Guard domestic cyber capabilities, the intent would be the same, as readiness reporting on cyber capabilities should be no different than any other domain. National Guard cyber units not on mission to USCYBERCOM are available for service tasks as well as being available for domestic response, similar to most other National Guard capabilities focused on domestic operations, to include JFHQ-State, the CBRN Response Enterprise and the National Guard Reaction Force (NGRF).

The National Guard's Defense Cyber Operations Elements (DCOE's) cyber defense units in each state, territory and the District, while technically not federally deployable under Title 10, are available potentially in support of defense to DOD Information Networks (DoDIN). As these units do not report readiness through their parent service in DRRS, the National Guard Bureau could potentially add them to the QRRC as a "domestic" capability. I will continue to work with the NGB to determine if this is the correct avenue for reporting this capability.

Again, we appreciate your unwavering support for the men and women of our Armed Forces. I am grateful for your attention to the status and availability of both the cyber mission forces on active-duty and those under the control and supervision of the National Guard Bureau and the Reserves. We will continue working with your staff, DoD and NGB to optimize real-time understanding of cyber forces availability and readiness.

Sincerely,

A handwritten signature in black ink, appearing to read 'M. Rogers', with a long horizontal flourish extending to the right.

MIKE ROGERS
Admiral, U.S. Navy
Commander