# “Hack the Pentagon” Fact Sheet - June 17, 2016

The “Hack the Pentagon” pilot, the U.S. Government’s first ever bug bounty, launched on April 18, 2016, and ran until May 12, 2016. Through this innovative effort, hackers were provided legal consent to perform specific hacking techniques against Department of Defense (DoD) websites, receiving financial awards for successfully submitting vulnerability reports. The pilot yielded impressive results, greatly exceeding expectations. DoD will capitalize on its success and continue to evolve the way we secure DoD networks, systems, and information.

The core purpose of the pilot was to improve the Department’s security. The U.S. Government is constantly under attack by hackers, and DoD is no exception. DoD information and networks have been compromised in the past through unpatched or unknown vulnerabilities in websites. Bug bounties are an effective means for private sector web and software developers to “crowdsource” security solutions at a fraction of the cost and time it would take to develop equivalent solutions in-house, while improving DoD network security.

The challenge was conducted against five public-facing websites: *defense.gov, dodlive.mil, dvidshub.net, myafn.net,* and *dimoc.mil*. The bug bounty challenge was hosted by HackerOne, a Silicon Valley-based firm that offers vulnerability disclosure and bug bounty as a service. Their online platform automates vulnerability triage and weeds out the noise, including duplicative reports. These functions normally take hundreds of man hours. HackerOne assisted in recruiting 1,410 participants for the challenge, and they generated a final total of 1,189 vulnerability reports. The total time it took to receive the first vulnerability report was only 13 minutes after the bounty began. Ultimately, 138 reports were deemed valid and unique security vulnerabilities which Defense Media Activity (DMA) quickly worked to remediate. The entire cost of the Hack the Pentagon pilot was $150,000, with about half going to the hackers themselves.

Although the pilot was a success, it only tested the crowdsourced security concept against public facing websites. We believe the concept will be successful when applied to many or all of DoD’s other security challenges. That’s why starting this month DoD is embarking on three follow-on initiatives. First, we will develop a vulnerability disclosure process and policy for DoD so anyone with information about vulnerabilities in DoD systems, networks, applications, or websites can submit it to us without fear of prosecution. Next we will expand bug bounty programs to other DoD Components, in particular the Services, by developing a sustainable DoD-wide contract vehicle. Lastly, we’ll include incentives in our acquisition policies and guidance so that contractors practice greater transparency and open their own systems for testing – especially DoD source code. With these efforts, we will capitalize on Hack the Pentagon’s success and continue to evolve the way we secure DoD networks, systems, and information.