Executive Summary:

- Direct U.S. Cyber Command, working in coordination with the National Security Agency, to conduct regular security reviews of weapons systems to identify vulnerabilities embedded in software and networks
- Require that source code for such weapons systems be made available on an ongoing basis for such testing; automate testing and require that any detected vulnerabilities are removed

Full Recommendation 4:

Proposal: Direct U.S. Cyber Command, working in coordination with the National Security Agency, to conduct regular security reviews of embedded software and networks for weapons systems to identify vulnerabilities. Require that source code for such systems be made available on an ongoing basis for such testing, and that any detected vulnerabilities are removed. The DoD should identify new standards and practices to eliminate system vulnerabilities, particularly those that require collaboration between the DoD and the defense industry.

Comment: The fundamental premise of this recommendation is that the technological advances in weaponry are now advances in software, not hardware; the measures to maintain and protect them must reflect that. In other words, a state-of-the-art fighter plane is a software system with wings, whereas previous fighters were planes with computers aboard.

Most modern weapons systems were designed under the assumption that their computing, networking, and software components were developed in controlled environments and that the security of these components would be maintained through adherence to standardized security procedures. As these systems have been integrated into increasingly networked environments, the safeguards designed to protect them have become inadequate. Conventional operational test processes are not evaluating the embedded code for vulnerabilities. Attempting to protect these systems by hiding them behind a network firewall is no longer sufficient to protect them.

Meanwhile, the sophistication of cyber-attacks has increased, rendering these weapons systems more vulnerable to attacks from direct infiltration, spoofing of sensors and interfaces, or more sophisticated systems-level attacks. For example, the use of older operating systems is one particular vulnerability that may be common in weapons systems that are not updated at a pace that matches modern commercial computing environments.

The Board recommends that U.S. Cyber Command and NSA have the best expertise on identifying vulnerabilities in the DoD, so this requirement should be added to their mission. These organizations should apply state-of-the-art automated vulnerability testing technology to continually safeguard the software code embedded in weapons systems.

Background: Vulnerability to hacking and infiltration is of paramount concern to all major companies, which conduct routine security reviews to identify and root out bugs or other vulnerabilities. Apart from internal reviews, Facebook, Dropbox, Microsoft, Twitter, Google, Yahoo, PayPal, Snapchat, Tesla, and GE are among companies that have hired outside hackers – or acquired companies that conduct

this work – to find vulnerabilities through “bug bounty” programs. These companies know that they will never find every vulnerability, so they solicit help from outside experts and white hat hackers.

In 2016, DoD instituted bug bounty programs of its own, such as Hack the Pentagon and Hack the Army, allowing anyone to search for and report vulnerabilities within the Pentagon and Army’s unclassified websites. Hack the Pentagon attracted 1,400 white hat hackers who discovered 138 vulnerabilities.

In addition, the Pentagon announced a new policy that allows anyone to report vulnerabilities to the Pentagon at any time, not just during exercises such as Hack the Pentagon. While this is an important step forward, there will always be vulnerabilities that will go overlooked, so it is important to consider more programs such as Hack the Pentagon and Hack the Army to enhance the visibility of these opportunities for white hat hackers. This has a complementary benefit of developing a potential recruiting pool of computer scientists with a sense of duty that DoD needs.

However, identifying vulnerabilities solves only part of the problem. Just as large modern companies update their software and corresponding systems as technology becomes more advanced, DoD must do the same. Otherwise, an even wider range of adversaries, criminals, and opportunists will be able to identify vulnerabilities and even sell them on the black market for zero-day bugs.