U.S. OFFICE OF SPECIAL COUNSEL
1730 M Street, N.W., Suite 300
Washington, D.C. 20036-4505

The Special Counsel

December 19, 2018

The President
The White House
Washington, D.C. 20500

Re: OSC File No. DI-17-3391

Dear Mr. President:

Pursuant to 5 U.S.C. §1213(e)(3), I am forwarding a report from the Department of the Navy (Navy) based on disclosures of wrongdoing at the Naval Air Warfare Center Weapons Division (NAWCWD), China Lake, California. The allegations were provided by [redacted] a program analyst and qualified Navy Joint Terminal Attack Controller, who consented to the release of his name. [redacted] disclosed that software known as KILSWITCH/APASS, developed and widely distributed by the Navy's Digital Precision Strike Suite (DPSS) had significant security vulnerabilities that could render it vulnerable [redacted].[1] Given the sensitive nature of the material, the Navy has designated the report as for official use only, and restricted further distribution pursuant to 10 U.S.C. §130e.

The investigation substantiated [redacted] allegations, finding that the software had significant cybersecurity vulnerabilities [redacted]

In response to these findings, the Navy directed the Chief of Naval Operations and the Commandant of the Marine Corps to ensure the software is only used with appropriate security measures in place. [redacted] Despite these corrective actions, significant concerns remain relating to the extensive and apparently unregulated distribution of the software, and the circulation of notice concerning its shortcomings.

[redacted] allegations were referred to Secretary of Defense James Mattis for investigation pursuant to 5 U.S.C. §1213(c) and (d). The Office of the Naval Inspector General investigated the matter, and Secretary of the Navy, Richard V. Spencer was delegated the authority to review and sign the report. [redacted] provided comments to the report on May 11, 2018.

PLEASE NOTE THE NAVY HAS DESIGNATED THIS INFORMATION AS FOR OFFICIAL USE ONLY AND FURTHER RESTRICTED DISTRIBUTION PURSUANT TO 10 U.S.C. §130E.

I strongly commend [redacted] for his public service in this matter. By filing this disclosure, he exposed a serious issue that potentially endangered the physical safety of forward-deployed military personnel. This software was widely distributed across [redacted], many of whom used it in combat. [redacted] should be lauded for his determination to protect the safety and wellbeing of military personnel who risk their lives to protect the United States.

I. Background

[redacted] alleged that the software was originally developed as [redacted] and as such was not subject to the oversight associated with formally recognized Department of Defense programs. Notwithstanding this status, he asserted that the program was impermissibly distributed and widely used by the Navy, Marine Corps (USMC), [redacted] He explained that the uncorrected security vulnerabilities were initially discovered in [redacted] during a review of the program's code. [redacted] noted that the software had been in use by forward-deployed U.S. units since [redacted], and emphasized the necessity of obtaining a full inventory of all distributed copies so that software updates could be executed and advising forward-deployed personnel to cease and desist the use of susceptible software.

II. Findings

The Navy's report explained that the software was developed [redacted], and [redacted] was used extensively by Navy and USMC personnel in operations. [redacted] These products, however, were never intended to be used in an operational setting by forward-deployed personnel. The report notes that "cybersecurity was not a concern for developers because they expected that the software would be used only for its intended purpose, [redacted], and would not be used widely in operations." Code analysis of the software, conducted as part of the investigation, indicated that they contained significant cybersecurity vulnerabilities.

Notwithstanding the development of these programs as a [redacted] lacking proper security controls, beginning in [redacted] the software was distributed and used by USMC, [redacted] The report notes that "thousands" of copies of the programs were loaded on to government issued and personally procured tablets. In some cases, the software was available for download on internal unit websites. [redacted]

[redacted]

Only [redacted] did the Marine Corps officially authorize the use of the software on government issued tablets for training and combat operations. [redacted] the Navy issued a series of similar orders permitting the use of the program by personnel. The report explained that there was also evidence that a significant number of USMC personnel used the software on personally procured devices that do not provide adequate security protections. [redacted]

The internal marketing of the software contributed to its widespread use. In [redacted], almost a year after initial security vulnerabilities were discovered, and only two weeks after widespread notification regarding software coding issues, NAWCWD's Director of Software and Mission Systems Integration sent an email solicitation regarding the software to [redacted] personnel featuring a variety of "inaccurate, incomplete, and misleading" assertions concerning the software's security. This email was then widely distributed across the entire [redacted]

III. Whistleblower Comments

[redacted] comments highlighted the poor internal controls that resulted in the distribution of unsecure, untested software to front-line personnel. He asserted that the programs at issue in this matter were marketed and showcased to secure political and capital gains for NAWCWD, with little regard for the consequences of rolling out vulnerable software to units that would rely on it in combat. [redacted]

IV. The Special Counsel's Findings

I have reviewed the original disclosure, the agency report, and [redacted] comments. While the report meets the statutory requirements, and the findings appear

reasonable, I have serious concerns about the lack of institutional oversight [redacted] facilitated the distribution of untested, unsecure proof of concept software to military personnel involved in combat missions. I urge the Navy to remain vigilant in ensuring that emergent software is properly vetted before distribution to military personnel.

It is clear, based on the information in the report, that the military maintains a complex process for the approval and evaluation of software used by military personnel. This process was totally circumvented here. The blatant disregard for procedure endangered the lives of military personnel. Accordingly, I also urge the Navy to conduct an accountability review of individuals who originally facilitated the distribution of this program [redacted] and take any disciplinary action it deems appropriate.

[redacted]

As required by 5 U.S.C. §1213(e)(3), OSC has sent copies of the agency report, this letter, [redacted] comments to the Chairmen and Ranking Members of the Senate and House Armed Services Committees. OSC has also filed redacted copies of these documents and a redacted copy of our original referral letter in our public file, which is available at www.osc.gov. This matter is now closed.

Respectfully,

Henry J. Kerner
Special Counsel

Enclosures

PLEASE NOTE THE NAVY HAS DESIGNATED THIS INFORMATION AS FOR OFFICIAL USE ONLY AND FURTHER RESTRICTED DISTRIBUTION PURSUANT TO 10 U.S.C. §130E.