Office of the Naval Inspector General

OSC DI-17-3391
NAVINSGEN 201702142

Report of Investigation

ALLEGED VULNERABILITIES OF THE KINETIC INTEGRATED LOW-COST SOFTWARE INTEGRATED TACTICAL COMBAT HANDHELD (KILSWITCH)/ANDROID PRECISION ASSAULT STRIKE SUITE (APASS) APPLICATION

27 March 2018

****

Table of Contents

Table of Contents ... i

Preliminary Statement ... 1

Information Leading to the OSC Tasking ... 1

Summary of Conduct of the Investigation ... 2

Summary of Findings of the Investigation ... 3

Summary of Allegations and Conclusions ... 3

Summary of Evidence Obtained During Investigation ... 4

ALLEGATION ONE ... 4

Findings of Fact ... 4

Discussion and Analysis ... 26

Conclusion ... 28

Recommendations ... 28

Actions Taken ... 28

Actions Planned ... 28

Personnel Actions Taken ... 28

ALLEGATION TWO ... 28

Findings of Fact 28

Discussion and Analysis 30

Conclusion 30

Recommendations 30

Actions Taken 30

Actions Planned 31

Personnel Actions Taken 31

OTHER MATTERS 31

Appendix A – Reference Documents A-1

Appendix B – Witness List B-1

Appendix C – Consolidated List of Recommendations C-1

Appendix D – Acronym List D-1

Office of the Naval Inspector General

OSC DI-17-3391
NAVINSGEN 201702142

Report of Investigation

ALLEGED VULNERABILITIES OF THE KINETIC INTEGRATED LOW-COST SOFTWARE INTEGRATED TACTICAL COMBAT HANDHELD (KILSWITCH)/ANDROID PRECISION ASSAULT STRIKE SUITE (APASS) APPLICATION

27 March 2017

****

Preliminary Statement

1. This report was prepared pursuant to a 5 June 2017 U.S. Office of Special Counsel (OSC) letter tasking the Secretary of Defense (SECDEF) to conduct an investigation under Section 1213 of Title 5 of the United States Code (5 U.S.C. § 1213).[i] SECDEF, in turn, directed the Secretary of the Navy (SECNAV) to conduct the investigation.

2. OSC is an independent federal agency whose primary mission is to safeguard the merit system by protecting federal employees and applicants from prohibited personnel practices. OSC also serves as a channel for federal workers to make allegations of: violations of law; gross mismanagement or waste of funds; abuse of authority; or, a substantial and specific danger to public health and safety.

3. Reports of investigations conducted pursuant to 5 U.S.C. § 1213 must include: (1) a summary of the information with respect to which the investigation was initiated; (2) a description of the conduct of the investigation; (3) a summary of any evidence obtained from the investigation; (4) a listing of any violation or apparent violation of law, rule, or regulation; and, (5) a description of any action taken or planned as a result of the investigation, such as changes in agency rules, regulations or practices, the restoration of any aggrieved employee, disciplinary action against any employee, and referral to the Attorney General of any evidence of criminal violation.

Information Leading to the OSC Tasking

4. The OSC tasking stems from a complaint to OSC alleging that the Naval Air Warfare Center Weapons Division (NAWCWD), Digital Precision Strike Suite (DPSS), developed and distributed two defective software applications (apps). More specifically, the tasking letter states that the Complainant, [redacted] asserts that the KILSWITCH and APASS apps have significant and uncorrected software vulnerabilities that were discovered [redacted] The Complainant further asserts that KILSWITCH and APASS are in use by DoD [redacted] While OSC advised that [redacted] consented to the release of [redacted] name, [redacted] is hereinafter referred to as the "Complainant."

5. The Complainant is a [redacted] [redacted] is also a [redacted] The Complainant [redacted] The Complainant [redacted] The Complainant was [redacted]

6. The OSC tasking letter stated:

> [Complainant] alleged that both KILSWITCH and APASS have significant uncorrected software vulnerabilities that were initially discovered [redacted] by PMA-281 [Strike Planning and Execution Systems program office], a program office within Naval Air Systems Command. . . . [Complainant] asserted that [redacted]

7. In addition to the OSC tasking letter, the Complainant asserted in an e-mail to us that the Navy Authority to Operate (ATO) the Electronic Kneeboard (EKB) with KILSWITCH, was improperly processed.[1] Specifically, he asserted that the Navy Approving Official (NAO), in deciding to issue the ATO, considered [redacted] certificate produced by the Naval Air Systems Command Defect Reduction Using Code Analysis (DRUCA) office asserting that it conducted static code analysis (SCA) of the KILSWITCH [redacted] and that [redacted] had [redacted] and [redacted] issues/defects. He stated: "This would not be appropriate documentation for an ATO application." We determined that the ATO was issued [redacted] and therefore, concluded that the NAO did not consider the certificate. We do, however, address this certificate in the Other Matters section of this report, below.

8. The OSC tasking letter stated the following allegations are to be investigated:

> (1) DPSS's KILSWITCH and associated APASS have significant security vulnerabilities; and
>
> (2) KILSWITCH/APASS vulnerabilities include [redacted]

Summary of Conduct of the Investigation

9. After receiving the OSC Tasking Letter, SECDEF tasked SECNAV to conduct the investigation. SECNAV, in turn, tasked the Office of the Naval Inspector General (NAVINSGEN) to conduct the investigation.

[1] EKB is discussed below.

10. At the outset of the investigative effort, the NAVINSGEN Investigating Officer (IO) interviewed the Complainant by telephone and received additional information by e-mail. Information provided by the Complainant that was not contained in the OSC tasking letter appears in the findings of fact, as appropriate.

11. During the course of the inquiry, the NAVINSGEN IO interviewed the Complainant and 29 witnesses. The NAVINSGEN IO also reviewed more than 100 documents, including applicable instructions and regulations, software test results, presentations, and e-mails.

Summary of Findings of the Investigation

12. We determined [redacted] KILSWITCH/APASS [redacted] currently being used in operations by U.S. military members.[2] [redacted] KILSWITCH/APASS [redacted] [redacted] KILSWITCH/APASS are designed to run on Android devices only. We further determined that KILSWITCH/APASS [redacted] software development applications. [redacted] software applications are intended [redacted] and not subject to the rigor of software development for programs of record. KILSWITCH [redacted] associated with a program of record. Devices on which KILSWITCH [redacted] was included were first fielded in [redacted] In this report, [redacted]

13. As discussed below, we found that KILSWITCH/APASS [redacted] have significant cybersecurity vulnerabilities. We further found that the potential impact of these vulnerabilities was never fully assessed [redacted] and such assessments are not required [redacted]

14. We found that authorized devices on which KILSWITCH/APASS run can effectively mitigate vulnerabilities. Both the Navy and the United States Marine Corps (USMC) issued ATOs that, if complied with, mitigate the cybersecurity vulnerabilities of KILSWITCH/APASS to varying degrees. [redacted]

15. We concluded that KILSWITCH/APASS [redacted] significant cybersecurity vulnerabilities. We also conclude that KILSWITCH/APASS [redacted] [redacted] We further concluded that KILSWITCH [redacted] is used by USMC on a device that effectively mitigates any potential vulnerabilities.

[2] KILSWITCH and APASS are two separate apps differentiated only by the user interface; the underlying software for both apps is nearly identical. We refer to KILSWITCH and APASS as "KILSWITCH/APASS" when discussing the underlying software, and individually as "KILSWITCH" and "APASS" when addressing the individual apps.

Summary of Allegations and Conclusions

16. Based on the intent of the OSC tasking letter and its preliminary review, NAVINSGEN decided to structure the allegations in a slightly different fashion than the OSC tasking. For Allegation One, we address whether versions of KILSWITCH/APASS [redacted] significant cybersecurity vulnerabilities. We also address whether the vulnerabilities are or were effectively mitigated. For Allegation Two, we address whether KILSWITCH/APASS [redacted]

Allegation One: That versions of DPSS's KILSWITCH and APASS that have been, and are currently, used in military operations and training have significant cybersecurity vulnerabilities that have not been effectively mitigated. **Substantiated.**

Allegation Two: That the KILSWITCH/APASS vulnerabilities [redacted] **Substantiated.**

Summary of Evidence Obtained During Investigation

ALLEGATION ONE

That versions of DPSS's KILSWITCH and APASS that have been and are currently used in military operations and training have significant cybersecurity vulnerabilities that have not been effectively mitigated. **Substantiated.**

Findings of Fact

17. [redacted] Defense Advanced Research Projects Agency (DARPA) created the Persistent Close Air Support (PCAS) program. KILSWITCH originally was a DARPA project for PCAS. [redacted] DARPA conducted its first successful demonstration of KILSWITCH [redacted]

18. DARPA transferred further development of KILSWITCH to NAWCWD and the Air Force Research Laboratory, Rome Labs (AFRL). NAWCWD and AFRL worked independently of one another to further develop their versions of a PCAS app. AFRL renamed its app the Android Tactical Assault Kit (ATAK).

19. Both KILSWITCH and ATAK were initially developed [redacted]

Operational Use of KILSWITCH/APASS

20. We determined that KILSWITCH/APASS has been used extensively by Navy and USMC personnel in operations [redacted] We considered information provided by users as well as documentary evidence.

21. In an e-mail dated [redacted] from DPSS Technical Director and Liaison Officer [redacted] [DPSS [redacted] to a Naval officer

working on the planned deployment of a carrier air group who was requesting information regarding KILSWITCH/APASS capabilities, the DPSS [redacted] attached a 3-page presentation, “KILSWITCH: Combat Proven by Marines [redacted][ii] Of note, the presentation stated the following:

- GOTS [Government Off the Shelf] mission planning/execution software application;
- Employed by Marines, [redacted] in combat during contingency operations since ≈[redacted]; and
- KILSWITCH has been employed in our Corps over past three years in the thousands.

22. When interviewed, the DPSS [redacted] stated that [redacted] did not know who prepared the briefing, but assumed it was DARPA.[iii] He also stated [redacted] thought he had seen the briefing before and that he could not attest to its accuracy because he believed it was “dated.” [redacted]

23. The DPSS [redacted] Regarding [redacted] KILSWITCH/APASS [redacted]

24. We spoke with the [redacted] who stated that KILSWITCH/APASS [redacted][vi] We discuss the [redacted] of KILSWITCH/APASS [redacted] in the Other Matters section of this report, below.

25. Based on witness interviews and our review of documents, we determined that KILSWITCH/APASS [redacted]

KILSWITCH/APASS Software Development

26. NAWCWD is an organization within the Naval Air Systems Command dedicated to maintaining a center of excellence in weapons development for the Department of the Navy. NAWCWD primarily operates in two Southern California locations: China Lake and Point Mugu.

27. DPSS is located at China Lake. It is a software development team that develops digital products used by Navy and Marine combat operating forces.

[3] We were unable to conclude [redacted]

28. Currently, the DPSS software development team consists of approximately 70 people. The team is made up of functional groups that address all areas of software development. Team personnel work on various software development projects and, for the most part, are not exclusively assigned to KILSWITCH/APASS development.

29. DRUCA is a division of NAWCWD. DRUCA performs SCA for software development at NAWCWD. As related to this investigation, DRUCA used two separate commercial tools to perform SCA; Hewlett-Packard (HP) Fortify (Fortify) and Klocwork Insight (Klocwork).

KILSWITCH/APASS Versions

30. For purposes of this investigation, [redacted] KILSWITCH/APASS [redacted]

- [redacted]
- [redacted]
- [redacted]

31. Both KILSWITCH/APASS [redacted][vii] The capabilities built into KILSWITCH/APASS [redacted]

32. KILSWITCH/APASS [redacted] Government-procured [redacted] tablets and phones and distributed to users for both training and combat operations. KILSWITCH/APASS [redacted] USMC [redacted] In addition to Government-procured tablets and phones, KILSWITCH/APASS was loaded by users onto personally procured Android devices.[4] A limited number of specially configured [redacted] tablets with KILSWITCH [redacted] by Navy [redacted] as part of the EKB program.

33. Currently, KILSWITCH [redacted] on a Marine Corps [redacted] Common Access Card [CAC]-controlled website.[5] In addition to KILSWITCH, the [redacted] site includes for download Navy and USMC ATOs that authorize the use of various government-procured devices, maps, and charts to load into KILSWITCH, user instructions, and a sample local command security policy letter and user agreement authorizing the use of Android tablets.

Static Code Analysis[ix]

34. SCA tools are used in software development to identify potential cybersecurity vulnerabilities in [redacted] The SCA tools that were used to analyze the

[4] We are unable to conclude that KILSWITCH/APASS [redacted]

[5] KILSWITCH v [redacted] from the [redacted] website.

KILSWITCH/APASS [redacted] were HP Fortify, Klocwork, and Infer. [redacted]

35. [redacted] The SCA tools pinpoint potential issues/defects [redacted] KILSWITCH/APASS [redacted] by DRUCA had up to nearly 500,000 [redacted]

36. SCA tools only identify potential cybersecurity vulnerabilities. Such potential vulnerabilities must be individually examined to determine whether the identified issue/defect is an actual vulnerability. The process of examining the potential vulnerabilities is called adjudication. Often during the adjudication process, the identified issue/defect is determined to not be an issue based on how the software is intended to be used or because the reported issue/defect is a "false positive." Actual issues/defects require that the software be corrected. Adjudication requires [redacted] over a period of time.

37. With regard to KILSWITCH/APASS, DRUCA engineers and DPSS developers worked together to address the identified potential vulnerabilities. However, DRUCA is responsible for the final adjudicated report.

38. In addition to an adjudicated SCA, developers may request an unadjudicated [redacted] An unadjudicated SCA is a single [redacted] in which the raw results of potential cybersecurity vulnerabilities are provided to the developer. There is no examination of the identified potential vulnerabilities by DRUCA with the developers. However, the scan report does provide the developers with some insight into potential vulnerabilities.

39. It is important to note that an unadjudicated [redacted] is of limited value. SCA only identifies potential issues/defects. Further, issues/defects identified by SCA are quantitative and not qualitative. For instance, [redacted] may be scanned in which hundreds of potential Critical or Priority 1 issues/defects are detected but after adjudication, the issues/defects may be proven to have no impact on cybersecurity. [redacted]

40. An adjudicated analysis is an iterative process with repeated scans and interactions between DRUCA engineers and DPSS software developers to address and correct identified issues or defects.

41. DRUCA process for adjudicating SCAs is:

[6] The STIG sets out minimum security standards that apply to any application or system used by the DoD to enhance security and minimize vulnerabilities.

- A DRUCA engineer [redacted] using the SCA tool and reviews all high level issues/defects in detail (Critical, High and some Medium). The engineer collaborates with software developer(s) to review all the defects identified by the SCA tool;

- Even though all defects regardless of severity are analyzed and reviewed, priority is placed on Critical and High defects as these are usually the issues/defects with most risk to the quality and reliability of a software product followed by Medium (Priority 3) and others;

- Each issue/defect is traced back to its original injection location, then discussed with developer(s) on why and how it could be of any impact;

- Factoring in the context, style, and requirement [redacted] as described by the developers(s), the DRUCA team provides recommendations on how the issue/defect should be resolved and avoided. Based on this discussion an issue/defect can be reclassified from higher to lower priority or vice-versa and then committed to be addressed as follows:

    a. Marked to be "Fix Now" (immediately),

    b. Marked as "Accepted" to be Fixed in later release (probable),

    c. Marked as "Review" for further investigation, and

    d. Marked as "Non-Issue/False-positive."

- At the conclusion of this adjudication phase, the developer(s) follow their own established software processes to address those defects that must be corrected. Additionally, they may work with their sponsors if there is a potential impact to cost or schedule for product release;

- Once corrective action has been taken by the development team, they may request that the DRUCA team perform another SCA scan to determine if the defect has been corrected and that no new defects have been introduced;

- If any new defects are identified during this correction process, the prior steps are repeated until no new corrective action is needed. The goal is to remove all adjudicated critical and high issues/defects reported by SCA tools and those medium defects that will cause functional impairment or cyber vulnerability. All other defects are addressed and scheduled accordingly with each program's Configuration Management process; and

- When a SCA is done that addresses all "must fix" issues/defects, an analysis report is provided. If the customer requests a certificate to show their sponsors, DRUCA will issue one. DRUCA does not issue certificates until the DRUCA team is satisfied that the software product addresses those defects marked for corrective action which includes all Critical and High defects.

42. DRUCA first issued a certificate attesting to the results of SCA in [redacted] for KILSWITCH[redacted] We discuss this certificate in the Other Matters section below.

43. DRUCA conducted two SCA scans for DPSS on the KILSWITCH/APASS [redacted] in February and [redacted] DPSS requested only a single [redacted] and the results were not adjudicated.

44. DRUCA conducted two unadjudicated SCA scans on KILSWITCH/APASS [redacted] [redacted] scan was conducted in response to this investigation and not for the purpose of [redacted] of KILSWITCH/APASS.

45. [redacted]USMC selected KILSWITCH/APASS as part of its Target Hand-Off System (THS) [redacted] [redacted]KILSWITCH/APASS [redacted] From approximately [redacted] the DPSS software developers worked on transitioning the KILSWITCH/APASS [redacted] KILSWITCH/APASS [redacted]

46. In support of its development of KILSWITCH/APASS[redacted] DPSS had DRUCA conduct three adjudicated SCAs. After each SCA, the KILSWITCH/APASS [redacted] was assigned a new [redacted] These [redacted] represented changes to the [redacted] based on the adjudicated SCAs. The SCAs were conducted from:

- [redacted] DRUCA conducted four Fortify [redacted]
- [redacted] DRUCA conducted five Fortify [redacted] and
- [redacted] DRUCA conducted four Fortify [redacted]

Concerns Raised Regarding KILSWITCH/APASS Quality

47. We found that in [redacted] when the Navy was seeking to implement an ATO for KILSWITCH, concerns regarding the quality of the KILSWITCH [redacted]We discuss below the ATO process for the Navy and USMC.

48. Program Management Activity-281 (PMA-281) is the Naval Air Systems Command (NAVAIR) program office responsible for the acquisition and life cycle management of a range of mission planning, control system, and execution tools that are developed and integrated in partnership with other NAVAIR program offices, other Services, and foreign nation customers/partners.

49. One of PMA-281's programs is EKB. EKB is a component of a Navy program of record. The goal for EKB is to provide an aviator with digital products, such as DoD flight information charts and instrument approach plates, tactical charts, and imagery. EKB [redacted] tablet. As part of the Navy ATO process, there was a requirement that KILSWITCH work within EKB.

50. E-mails beginning in [redacted] and current witness interviews, establish that as part of the ATO process, NAVAIR personnel requested that DPSS send them the KILSWITCH [redacted] as well as SCA and Information Assurance (IA) data.

51. Beginning on [redacted] PMA-281 specifically requested the SCA report for KILSWITCH [redacted][i] We note that at the time, there had not been any SCA (adjudicated or unadjudicated) of KILSWITCH/APASS [redacted] Rather, DRUCA had conducted two unadjudicated, single SCA scans of KILSWITCH/APASS [redacted] in [redacted]

52. On [redacted] the DPSS [redacted] responded that "the Fortify scan and report takes a concerted effort and is underway with a team at [DRUCA]." A PMA-281 member responded that day, to the DPSS [redacted] that they needed the "raw HP Fortify output file."

53. On [redacted] the DPSS Program Manager responded to the e-mail and informed a PMA-281 member that he expected the SCA results that afternoon. The DPSS Program Manager added, "some of our SME's [subject matter experts] have brought up that without having our people that wrote the application going through this with you there might be some misunderstandings of the reads."[xii] The PMA-281 member responded that after they reviewed the SCA report "we'll circle back with any questions."[xiii]

54. On [redacted] the DPSS [redacted] wrote to the PMA-281 member that both the NAWCWD legal counsel and the Marine KILSWITCH program of record sponsor "want us to only provide you the audited results."[xiv]

55. A partially adjudicated report dated [redacted] [[redacted] SCA Report] was prepared by DRUCA.[xv] This report is different from the "raw" Fortify output file that the PMA-281 member requested on [redacted]

56. On [redacted] after further e-mails regarding release of the SCA report, the DPSS Program Manager provided the [redacted] SCA Report to PMA-281 in response to its request for the raw SCA data.

57. After reviewing the [redacted] SCA Report, on [redacted] the NAVAIR Chief Information Office, Technical Director sent an e-mail to PMA-281 personnel and other NAVAIR personnel in which he wrote: "Wow. . . . I have huge concern with all these high, medium, and lows [issues/defects]."[xvi]

58. The [redacted] SCA Report is 1,277 pages long and partially adjudicated. The report included the identified issues and "snippets" of code related to those issues. The Report Overview states:

> A total of 5,269 issues were uncovered during the analysis. This report provides a comprehensive description of all the types of issues found in this project. Specific examples and [redacted] are provided for each issue type.

59. The Report Overview listed the following issues with the reported number of findings:

- 0 Critical;
- [redacted]
- [redacted]
- [redacted]
- 735 Don't Care;
- 1 False Positive; and
- 186 External Issues.

60. [redacted]

61. To assist with reviewing the KILSWITCH [redacted] PMA-281 obtained assistance from the Applied Physics Lab (APL) and provided it the [redacted] SCA Report for its review.[7][xvii]

62. In [redacted] APL prepared a PowerPoint presentation regarding its review of the [redacted] SCA Report. In its report, APL addressed some of the findings from the [redacted] SCA Report. APL also noted that since the [redacted] was not provided "there was insufficient scope to validate real or perceived flaws/vulnerabilities." APL also wrote that in order to better analyze KILSWITCH; [redacted] was required.

63. Sometime in [redacted] DPSS provided the [redacted] for KILSWITCH/APASS [redacted] to PMA-281. PMA-281, in turn, gave the [redacted] to APL for SCA. KILSWITCH/APASS [redacted] was provided because DPSS [redacted] and was no longer working with KILSWITCH/APASS [redacted]

64. In a PowerPoint presentation, dated [redacted] APL reported the findings of its SCA of the KILSWITCH/APASS [redacted][xviii] For its analysis, APL used the Klocwork and Infer tools. In the presentation, APL reported there were [redacted] findings using Klocwork and [redacted] using Infer. APL addressed some of the specific findings and provided recommendations for moving forward with KILSWITCH/APASS [redacted] software development.

65. APL's comments include:

- Critical issues persist that should be corrected;

[7] APL is a University-Affiliated Research Center Laboratory (UARC) associated with Johns Hopkins University. UARCs are not-for-profit entities sponsored and primarily funded by the U.S. Government to address technical needs that cannot be met as effectively by existing government or contractor resources. The DON is APL's primary sponsor. APL's assistance was provided pursuant to an omnibus contract with NAVSEA.

- Many issues [redacted] of KILSWITCH [redacted] have been corrected, but other new issues have replaced them;

[redacted]

66. APL recommended that DPSS, PMA-281, and APL engage in discussions and that DPSS [redacted] which would correct deficiencies in KILSWITCH/APASS by [redacted]

67. On [redacted] DPSS, PMA-281, and APL held their first formal team meeting to discuss a proposed path forward, which included APL support for software development process improvement and for an independent evaluation and Independent Verification & Validation (IV&V).

68. In [redacted] DRUCA conducted SCA of the KILSWITCH/APASS [redacted] [redacted] using Fortify and Klocwork. In [redacted] DRUCA provided a report of its findings to PMA-281. In its report, DRUCA stated that after adjudicating the SCA reports, there were [redacted] and [redacted] findings. DRUCA explained in the report how it came to its conclusions.

69. In [redacted] APL's Software Assurance Research & Applications (SARA) Lab independently analyzed KILSWITCH/APASS [redacted] using Klocwork and an additional SCA tool, Infer. APL drafted a report of its findings, and addressed DRUCA's January report that was provided to PMA-281.[xix]

70. APL reported that Klocwork detected 5,908 findings which included [redacted] and [redacted] findings.

71. In its report, APL wrote:

- The objective of the work discussed in this paper is twofold. The first is to determine the extent to which [redacted] in light of the information provided in [DRUCA's [redacted] report of [redacted] and [redacted] findings]. The second objective is to provide, based on the SARA Lab's expertise, an assessment of the overall quality of the [redacted] and recommendations for improvement;

- In this case, we arrived at the conclusion that real weaknesses do still exist [redacted] including priority 1&2 issues that were not discussed in [DRUCA's [redacted] report];

- It is our assessment that the KILSWITCH [redacted] [redacted] is of insufficient quality for operational production software and needs to be reworked or rewritten using best practices for software engineering and software assurance; and

- We conclude that KILSWITCH likely has serious problems, which may result in security vulnerabilities or operational failures [redacted]

72. APL's SARA Lab also reported that the Infer tool detected 359 "memory based issues." Regarding the memory based issues, SARA Lab wrote: "All of these are the sorts of errors that could lead to either the application [redacted][xx]

73. In [redacted] PMA-281 had computer scientists from Software Engineering Institute (SEI) join APL to provide further outside software engineering expertise.[8] In [redacted] SEI conducted an independent analysis of the KILSWITCH/APASS [redacted] [redacted] SEI's results were consistent with APL's.

74. On [redacted] SEI briefed APL on its independent findings and analysis of the KILSWITCH/APASS [redacted]. SEI and APL agreed on the overall quality of the KILSWITCH/APASS [redacted] assessed that "major additional 'rework' is necessary to achieve the threshold level Mission Critical code."

75. On [redacted] APL presented a "KILSWITCH Way-Ahead Decision Brief" to PMA-281.[xxi] In its briefing, APL reported SEI's independent assessment of the KILSWITCH/APASS [redacted]. It noted:

- That both APL and SEI performed independent analyses without knowledge of each other's approaches or existing findings;

- Analyses agree overall on the quality, security, modularity, sustainability, documentation, etc., of the [redacted];

- Concurrence also achieved on the complexity of the [redacted], rendering a complete redevelopment effort infeasible; and

- [SEI and APL] assess that this is a classic case [redacted] turned production.

76. APL recommended a KILSWITCH Tiger Team be established. By this, they envisioned APL and SEI working with DPSS's development team and DRUCA to improve software development practices. This recommendation was not implemented, and the [redacted] course of action of [redacted] remained in place.

77. In [redacted] in response to written questions from the NAVINSGEN IO, APL provided written answers.[xxii] Regarding the software development practices by DPSS that APL observed, APL stated:

[8] SEI is a Federally Funded Research and Development Center (FFRDC) associated with Carnegie Mellon University. FFRDCs are not-for-profit entities sponsored and primarily funded by the U.S. Government to address technical needs that cannot be met as effectively by existing government or contractor resources. The U.S. Army is SEI's primary sponsor.

> It is noteworthy that in our conversations with DPSS throughout this engagement, we have been informed that KILSWITCH was a rapidly developed prototype app [redacted] which did not properly derive and decompose requirements as would be expected with production software projects. Most of their application functional requirements were received informally via phone or email, [redacted] and then never documented. . . . The lack of requirements and documentation is incongruent with standard software engineering principles and best practices.

78. And:

> Furthermore, conversations with the developers revealed that standard software development practices such as documentation, unit testing, and [redacted] were either entirely or almost entirely lacking.

79. And:

> At the time of our [[redacted] analysis report, we were not aware of any documentation related to KILSWITCH apart from a one-page PowerPoint slide that was produced by DPSS in [redacted] that showed a high-level block diagram of the components of KILSWITCH. In phone conversations with DPSS Software Technical Lead in early [redacted], [he] mentioned that [DPSS] did not have much in the way of documentation related to KILSWITCH.

80. And:

> We were told as recently as [redacted] by [DPSS's Software Technical Lead] that requirements for KILSWITCH were received informally via phone or email and never documented, so there is no document detailing the requirements for KILSWITCH. In our visit to DPSS in [redacted] we discussed the lack of documentation with [DPSS's Software Technical Lead] and others from DPSS and were told that some limited documentation was under development at that time, such as Coding Standards and Change Management Processes. Upon PMA-281's request, a PowerPoint slide deck consisting of 8 slides titled "DPSS KILSWITCH Module Overview" was produced by DPSS on [redacted] We have seen a few documents related to user's guides and training materials for the KILSWITCH app, but to this point have not seen much regarding documentation of KILSWITCH development.

81. Regarding APL's statement in its [redacted] analysis report of its "assessment that the KILSWITCH [redacted] and development environment is of insufficient quality for operational production software," we asked APL for further comment. It stated:

> Our assessment of the [redacted] of KILSWITCH is consistent with the comments by [DPSS Software Technical Lead] from DPSS on [redacted] This level of quality may be acceptable for prototypes and very limited deployments (i.e., in time-limited special operations

> scenarios), but we assess that greater rigor is needed for widely deployed operational software for DoD.

82. Regarding standards to which software should be developed, APL stated:

> APL also recognizes that the DoD currently holds [software for] commercial mobile devices to a somewhat different standard than [software] in other environments. For example, production software that is considered a primary point of reference, safety critical, mission critical, and/or software that is installed on permanent aircraft equipment undergoes substantial scrutiny related to the quality, reliability, maintainability, survivability, resiliency, etc., and KILSWITCH (by nature of being a mobile app) does not fall under existing policy and practice. Therefore, the standards to which we hold other acquired software do not yet transcend into the mobility solution space.

83. Regarding APL's statement in its [redacted] analysis report that "KILSWITCH likely has serious problems, which may result in security vulnerabilities or operational failures (e.g., crashes or unexpected behavior)," we asked APL for further comment. It stated:

> In order for APL to conclude that KILSWITCH "has" serious problems, the team would require an in-depth understanding of the deployment and usage of the KILSWITCH app. We identified many real issues [redacted] but could not evaluate them in the greater context of how these issues may be manifested during operational use of the app. Security vulnerabilities are highly dependent on how and where the software is used [redacted] there was sufficient cause for concern to warrant the comment that KILSWITCH *likely* has serious problems.

84. As to the status of KILSWITCH/APASS [redacted] as of [redacted] APL informed us that it has seen positive movement by DPSS [redacted][xxiii] APL stated:

> Although there remain a number of issues that still need to be addressed, a scan of KILSWITCH [redacted] did reveal that fixes were being implemented resulting in a reduction [of issues] being reported by Klocwork. Additionally, since then, APL and SEI have received some documentation from DPSS through PMA-281. This included a Configuration Management Plan (CMP), Software Requirements Specifications (SRS) and traceability, Architecture diagrams and a Software Development Plan (SDP). The development of these documents is additional evidence of progress being made in the transition from an [redacted]

85. APL, SEI, DPSS, and DRUCA continue to attend weekly technical meetings to discuss the issues that APL and SEI believe need to be addressed to attain the highest [redacted]

86. The DPSS Deputy Program Manager (DPSS DPM) has been in that position for approximately 3 years.

87. The DPSS DPM acknowledged that KILSWITCH/APASS [redacted] and that he was not aware of "any formal process or documentation specifically that was put in place."[xxiv] He added that many of DPSS's research and development projects "don't follow a formal process by design because they want you to go off and think in the art of possible, not what is formally written down."[xxv] The DPSS DPM told us that KILSWITCH/APASS [redacted] and there was no expectation that it would become operational.[xxvi]

88. The DPSS DPM stated that [redacted] in which "you do whatever you need to do to figure out whether or not your idea is even feasible."[xxvii] He added:

> Once you have [redacted] then people can make the determination on whether or not they want to proceed, and they can implement that type of idea [redacted] how they want to proceed.[xxviii]

89. The DPSS DPM stated that up until late-[redacted] DPSS was exclusively an [redacted] organization.[xxix] However, since that time, DPSS has transitioned to conducting [redacted] software development [redacted] software development.

90. The DPSS DPM stated that KILSWITCH [redacted] He explained that in mid-[redacted], the USMC decided to fund KILSWITCH/APASS as a [redacted] for the Marine Corp's Target Hand-off System [THS]. At that time, DPSS [redacted] KILSWITCH/APASS [redacted][xxx] He added that [redacted] "we then went in and adhered to all of the formal processes associated with developing software [redacted] [redacted][xxxi]

91. The DPSS DPM also stated that KILSWITCH [redacted] was tested for cyber vulnerabilities by the USMC at its cyber range testing facility. He also stated [redacted] KILSWITCH is loaded.[9] Importantly, he noted that the cyber security attributes of KILSWITCH [redacted] were not [redacted] KILSWITCH. He stated:

> [redacted] It may have some similar, but they would not be the same, [redacted][xxxii]

92. Regarding potential cybersecurity vulnerabilities [redacted] KILSWITCH [redacted] the DPSS DPM stated:

[9] We address [redacted] Marine Air Ground Tablet ATO.

> So yes, there are, I am certain that there are potential. And again, I keep coming back to the word “potential,” because the [SCA] findings mean -- doesn’t mean that there are security vulnerabilities, it means that there is a potential for one. And there are plenty of potential [cyber]security vulnerabilities [redacted]

93. [redacted]

94. Regarding potential cyber vulnerabilities [redacted] the DPSS DPM stated that the intended use [redacted] He added: [redacted]

95. With regard to [redacted] the DPSS DPM stressed that [redacted] [redacted] based on requests from various customers for different functionalities. [redacted] [redacted] and not intended as such. Further, the DPSS DPM stated that the developers could not know whether the software was used in ways other than how it was intended.

96. The DPSS DPM addressed the issue of APL’s SCA of KILSWITCH/APASS [redacted] and characterized it as “a huge findings list without adjudication.”[xxxv] He stated APL’s assessment of the [redacted] and potential security concerns was subjective.[xxxvi] He added that DPSS and APL have worked together to address APL’s concerns. He stated that the KILSWITCH development team, DRUCA, and APL have addressed all the issues identified in the SCA reports and all agree that all critical and high findings have been adequately addressed.

97. Regarding working with APL, the DPSS DPM said that the KILSWITCH development team had gained from the experience but that it did not affect its processes. He stated:

> We can’t become [redacted] and produce a better product if we’re kept in the dark on what makes things better. So it then became a collaborative effort where APL would coach us on what they would like to see. Quite honestly, we were on -- and they have made this public as well, we were on that corrective path anyway. We have not -- to this date, we have not made any corrections in software development processes or [redacted] as a finding of APL.[xxxvii]

98. Regarding becoming [redacted] to produce a better product, we did note that on [redacted] DPSS published a 60 page document, “DPSS Coding Standard.” This is the first published [redacted] Standard for DPSS.

99. The DPSS DPM stated that based on work that has been done on the KILSWITCH [redacted] since APL became involved, “we have changed KILSWITCH significantly” and these changes [redacted] “make it better and more secure.”[xxxviii] KILSWITCH [redacted]

100. The DPSS DPM stressed that KILSWITCH is built as part of a system. He added that cybersecurity relies on the KILSWITCH app, the operating system on which it is run, and the hardware on which it is loaded.

101. Regarding potential cyber vulnerabilities in KILSWITCH/APASS [redacted] the DPSS DPM stated:

> I believe that the risk of those vulnerabilities being exploited was minimal due to the intended disconnected nature of the devices using the application. If the devices were connected to anything at all, they would have been connected to an encrypted . . . radio which would have provided intrusion protection via the encryption.[xxxix]

KILSWITCH/APASS Authorities to Operate

Marine Corps Authorities[xl]

102. The Marine Corps Approving Official (MCAO) signed two ATOs for mobile devices, dated [redacted]

- AUTHORIZATION TO OPERATE (ATO) ANDROID TABLET (ANTAB) STATE ZERO IN THE UNITED STATES MARINE CORPS (USMC) COMBAT AND IN COMBAT OPERATIONS: [redacted]-0002 (ANTAB ATO, State Zero)[xli]

- AUTHORIZATION TO OPERATE (ATO) AND CONNECT (ATC) ANDROID TABLET (ANTAB) STATE ONE IN THE UNITED STATES MARINE CORPS (USMC) COMBAT AND IN COMBAT OPERATIONS: [redacted]-0001 (ANTAB ATO, State One-0001)[xlii]

ANTAB ATO, State Zero

103. The ANTAB ATO, State Zero authorized USMC personnel to use "government owned" ANTABs for training and combat operations. ANTABs are commercially available tablets running the Android operating system with no required modifications. Approximately 600 government-procured ANTABs loaded with KILSWITCH/APASS [redacted] have been issued.

104. The ATO authorized using ANTABs for data classified [redacted] The ATO provided that the ANTAB [redacted] The ATO prohibited connecting ANTAB devices to the Marine Corps Enterprise Network. The ATO is set to expire on [redacted]

105. The ATO [redacted] [redacted] The issued ANTABs do not have the wireless, cellular, or Bluetooth connections disabled.

106. The ATO required that the “system owner” develop and submit a Plan of Action and Milestones within 14 days and complete the Marine Corps Certification and Accreditation Tool (MCCAST) package within 60 days [10] Neither of these requirements were met.[xliii]

107. The ANTAB ATO, State Zero states that the overall risk of the ANTAB is “High.” The ATO stated: “This High risk is due to unknown vulnerabilities as no comprehensive risk assessment has been conducted on the device.”

ANTAB ATO, State One

108. The ANTAB ATO, State One-0001 authorized USMC personnel to use “government owned” ANTABs for training and combat operations. It authorized the use of the ANTAB [redacted] subject to constraints on the type of data listed in the ATO. The ATO prohibited connecting ANTAB devices to the Marine Corps Enterprise Network. Forty-six ANTABs with State One configuration were issued to USMC personnel for operational use. A smaller number of additional ANTABs were issued for use in training.

109. The ATO also required that any wireless, cellular, or Bluetooth connections be disabled. We determined that this requirement was built into the devices.

110. The ANTAB ATO, State One permitted data transfer between devices using secure methods.

111. The ATO required the “system owner” to:[11]

- complete a White Team assessment to determine full scope of risk associated to the ANTAB State One within 45 days; and[12]
- complete the MCCAST package within 60 days.

112. These requirements were not met.[xliv]

113. The ATO was superseded on [redacted]

Superseding ANTAB ATO, State One[xlv]

114. The MCAO signed an ATO, dated [redacted] AUTHORIZATION TO OPERATE (ATO) AND CONNECT (ATC) ANDROID TABLET (ANTAB) STATE ONE IN THE UNITED STATES MARINE CORPS (USMC) COMBAT AND IN COMBAT OPERATIONS: [redacted]-0001-2 (ANTAB ATO, State One-0001-2). This ATO will expire on [redacted]

[10] MCCAST is a data management tool in which cybersecurity records and artifacts are stored and accessed to assist USMC and Navy accreditation authorities and information systems officers ensure compliance with Information Assurance standards.

[11] A system owner is the office responsible to for the material management (budgets, purchasing, etc,) of a system. There is no “system owner” for ANTAB.

[12] A white team is a group responsible for refereeing an engagement between a Red Team of mock attackers and a Blue Team of actual defenders of information systems.

115. ANTAB ATO, State One-0001-2 superseded ANTAB ATO, State One-0001. [redacted]

116. ANTAB ATO, State One-0001-2 also required that the ANTAB devices [redacted]

117. [redacted] It is authorized for DoD applications by DoD STIGs.

118. Significantly, we note the Marine Corps never required DPSS to make KILSWITCH/APASS function in the [redacted] Rather, USMC contracted a commercial entity to modify settings on the KILSWITCH/APASS app so that it would work in the [redacted] Each of the 46 State One configured ANTABs designated for operational use was reconfigured so that KILSWITCH/APASS functioned in the [redacted] in conformance with the ANTAB ATO, State One-0001-2. At this time, the wireless, cellular, or Bluetooth connections were disabled by administrator action and could not be enabled by users.

119. The Marine Corps Aviation action officer [redacted] The majority of these tablets have KILSWITCH/APASS loaded onto them. The Action Officer for the Marine Corps Deputy Commandant for Aviation believes that the vast majority of these tablets were used consistent with the ANTAB ATO, State Zero and that if classified data was loaded onto the device, the device was thereafter treated as any other classified item and the tablet was properly stored and controlled and that the owner surrendered the device to Marine Corps control.

120. ANTAB ATO, State One-0001-2 required the "system owner" to:[13]

- complete a White Team assessment to determine full scope of risk associated to the ANTAB State One within 45 days, and
- complete the MCCAST package within 60 days.

121. These requirements were not met.[xlvi]

Marine Corps Certified Application: KILSWITCH[xlvii]

122. The MCAO signed a memorandum, dated [redacted] "MARINE CORPS CERTIFIED APPLICATION (MCCA): KINETIC INTEGRATION LIGHTWEIGHT SOFTWARE INDIVIDUAL TACTICAL COMBAT HANDHELD (KILSWITCH) [redacted] (KILSWITCH MCCA). The MCCA authorized KILSWITCH to operate on ANTABs in accordance with the ANTAB State Zero and State One-0001ATOs.

[13] There is no "system owner" for ANTAB.

123. When the KILSWITCH MCCA was implemented, KILSWITCH [redacted] The MCCA applied to KILSWITCH [redacted]

124. In the KILSWITCH MCCA, the MCAO authorized an "exemption of certification and accreditation" for KILSWITCH. The memorandum further states:

> Per ICSD 018 [Marine Corps Certification and Accreditation Process] the Marine Corps AO will certify applications, after verification that ensures the application does not require modifications to its hosting system [redacted]

125. Accordingly, the KILSWITCH MCCA exempts KILSWITCH from the USMC certification and accreditation process.

126. The KILSWITCH MCCA further states:

- the KILSWITCH Program Manager must complete the project in MCCAST within 90 days,

- the project is required to have the technical artifacts, to include a Validation against a standard baseline system, and

- the application must be registered within the Department of the Navy (DON) Application and Database Management System (DADMS) within 60 days.

127. The MCCA also stated: "Failure to complete these actions will result in the termination of this MCCA and the application will be placed on the Unauthorized Software List determined that the above required actions were not completed." The MCCA does not have a termination date.

128. We determined that the three actions required by the KILSWITCH MCCA were not taken. However, the KILSWITCH MCAA was not terminated and KILSWITCH was not placed on the Unauthorized Software List. [xlviii]

Target Hand-off System (THS) ATO[xlix]

129. The MCAO signed an ATO, dated [redacted] AUTHORIZATION TO OPERATE (ATO) AND CONNECT TARGET HAND-OFF SYSTEM (THS) TO THE MARINE CORPS ENTERPRISE NETWORK SECRET IP ROUTER NETWORK (MCEN-S): [redacted]-1298 (THS ATO). This ATO will expire on [redacted]

130. THS is a tablet-based system [redacted] Communications between devices is over secure methods.

131. THS incorporates KILSWITCH [redacted] into the THS system. In [redacted] Marine Corps Systems Command conducted testing of THS at the USMC cyber range. The ATO

required that an IV&V be conducted within 90 days of the signing of the ATO and that failure to conduct the IV&V could result in termination of the ATO. This IV&V was never performed.

132. As discussed above, KILSWITCH [redacted] Further, as discussed above, three separate SCA analyses were conducted by DRUCA on KILSWITCH [redacted] to address potential cybersecurity vulnerabilities. While we address concerns regarding the potential cybersecurity vulnerabilities of the KILSWITCH [redacted] [redacted] below, we found that the MCAO determined the THS system has adequately mitigated those vulnerabilities to a reasonable and acceptable level.

133. As of [redacted] 36 THS tablets have been issued for testing and training.

Marine Air Ground Tablet ATO[l]

134. The MCAO signed an ATO, dated [redacted] AUTHORIZATION TO OPERATE (ATO) THE MESH NETWORK MANAGER (MNM) MARINE AIR GROUND TABLET (MAGTAB): [redacted]-0705 (MAGTAB ATO). This ATO will expire on [redacted]

135. The MAGTAB is a [redacted] that allows users to connect with other MAGTAB users through secure communications. The ATO permits users to transfer data from one MAGTAB to another MAGTAB by secured communications methods. MAGTABs host various applications, including KILSWITCH [redacted] The MAGTAB employs [redacted]

136. A Security Assessment Report (SAR) and IV&V of the MAGTAB was conducted in [redacted] prior to the issuance of the MAGTAB ATO.[li] As part of the IV&V, applications that are loaded onto the MAGTAB were tested by an Independent Verifier.[14] The testing included SCA of the [redacted] for the applications. The MAGTAB IV&V lists KILSWITCH [redacted] as an application on the MAGTAB. The IV&V also assessed whether data on the device, including KILSWITCH data, was accessible to other than authorized users.

137. Evidence we developed established that KILSWITCH [redacted] was not tested with SCA tools prior to the issuing of the MAGTAB ATO. We received evidence that DPSS withheld the [redacted] from the Independent Verifier so SCA could not be performed. Accordingly, we are concerned that KILSWITCH [redacted] was approved for the MAGTAB, and is in fact included as an application on the MAGTAB, without being properly assessed for cybersecurity vulnerabilities.

138. We note that the Independent Verifier addressed concerns arising out of its SCA of the ATAK app.[15] The Independent Verifier [redacted] findings using the Fortify tool. Also, the Verifier was able to detect "leakage" of data outside the [redacted] of information loaded into ATAK.[16] The Independent Verifier recommended removing ATAK from the acceptable applications for MAGTAB until the identified issues were

[14] Independent Verifier was a commercial entity on contract with the Marine Corps System Command.

[15] As we noted above, ATAK is an application that provides similar functions to KILSWITCH/APASS and was developed by Air Force Research Laboratory.

[16] Data that leaks outside the [redacted] is potentially susceptible to unauthorized access and manipulation.

properly addressed. The Independent Verifier also stated that the risk associated with ATAK "will be tough for the [MC]AO to accept." We noted that the identified ATAK issues were addressed with the developers and corrected. Subsequent to the correction, ATAK was loaded onto the MAGTABs as one of the available applications for users.

139. We further noted that the Independent Verifiers did not detect any vulnerabilities with KILSWITCH/APASS in its assessments of the MAGTAB itself. Accordingly, there is evidence that the [redacted] effectively mitigates the potential cybersecurity vulnerabilities associated with KILSWITCH/APASS [redacted]

140. To date, 1,260 MAGTABs have been issued for training and operations.

Navy Authorities

141. The NAO issued three authorities that permitted limited use of KILSWITCH by Navy personnel. These were:

- INTERIM AUTHORIZATION TO TEST (IATT) THE KINETIC INTEGRATION LIGHTWEIGHT SOFTWARE INDIVIDUAL TACTICAL COMBAT HANDHELD (KILSWITCH [redacted] (Navy IATT);

- INTERIM AUTHORIZATION TO OPERATE (IATO) THE KINETIC INTEGRATION LIGHTWEIGHT SOFTWARE INDIVIDUAL TACTICAL COMBAT HANDHELD (KILSWITCH) [redacted] (Navy IATO); and

- AUTHORIZATION TO OPERATE (ATO)/TYPE ACCREDITATION THE ELECTRONIC KNEEBOARD CONFIGURATION (EKB-CONFIG) [redacted] (Navy ATO).

Navy IATT[lii]

142. The NAO signed the IATT which authorized [redacted] KILSWITCH [redacted] The IATT states that the purpose for the granted authority was "to test the compatibility and interoperability of the [redacted] hardware and KILSWITCH and APASS software while deployed in [redacted] situations."

143. The IATT was in force from [redacted] It required the devices on which KILSWITCH was loaded to remain in "Airplane Mode" to disable the wireless, cellular, or Bluetooth connections, and GPS. The IATT authorized up to [redacted] on the tablet. Further, the IATT stated that users were required to comply with [redacted] Further, the IATT stated that users were required to comply with [redacted]

144. [redacted] KILSWITCH (KS) Concept of Operations (CONOPS)," [redacted]

[redacted]

145. [redacted] said that he learned about KILSWITCH during the work up for an upcoming deployment from a junior officer who had been assigned as an instructor at the [redacted] He said that the officer told him that while at [redacted] briefed the [redacted] about their experiences using KILSWITCH operationally [redacted][liii] Based on the briefing, the junior officer recommended KILSWITCH to the [redacted] for the upcoming deployment.

146. [redacted] worked with the NAO to prepare the CONOPS and to obtain the IATT. With regard to the value of KILSWITCH, [redacted] stated: "On a scale from 1 to 10, I'd rate it 11."[liv]

Navy IATO[lv]

147. [redacted]

The IATO states that the purpose for the granted authority was "to allow continued operations of KILSWITCH [redacted] to meet mission requirements and to allow for completion of Certification & Accreditation/Assessment & Authorization activities." The IATO was in force from [redacted]

148. The IATO required that use of KILSWITCH past the termination date of the IATO "must be authorized via NAVAIR sponsored EKB."

Navy ATO[lvi]

149. The NAO signed the ATO on [redacted] It authorized the use of EKB [redacted] The ATO stated: "Use of KILSWITCH capability is only authorized via NAVAIR sponsored EKB." The ATO states that it expires on [redacted] or sooner.

150. PMA-281 required that all applications run on EKB must run in the [redacted] As discussed above, DPSS was never provided funding [redacted] so that KILSWITCH would work in the [redacted][17] On [redacted] the DPSS [redacted] sent an e-mail on which a PMA-281 member was cc'ed, noting that [redacted] He wrote:

> This is potentially a show stopper. [redacted]

[17] As discussed above, KILSWITCH does work in the [redacted] The USMC contracted with an outside commercial entity to modify the app so that it would work in the MAGTAB.

151. The Commander, PMA-281 stated that the former-Commander, PMA-281 was briefed about the [redacted] issue and that the former-Commander "verbally instructed the PMA-281 team to accept this risk for now; move KILSWITCH out of the [redacted] for the [redacted] with the understanding this fix was a high priority for DPSS to provide to PMS-281."[lvii]

152. The Commander, PMA-281 assumed his position on [redacted] and continued the previous commander's approach of having PMA-281 work with APL and DPSS to implement corrections to the KILSWITCH [redacted] Factors that the current commander considered in making his risk assessment were that the EKB tablets with KILSWITCH [redacted] Additionally, only 60 tablets were released for use.

153. We note that not until [redacted] DPSS received approximately $200,000 from PMA-281 to modify the KILSWITCH/APASS [redacted] This was the first time that DPSS was funded to have KILSWITCH/APASS [redacted] On [redacted] DPSS [redacted] PMA-281. PMA-281 determined that the modification did not satisfy its requirements.

154. In mid-[redacted] the NAO was informed that KILSWITCH [redacted] Representatives from PMA-281, DPSS, APL, NAVAIR, and NAO's office met on [redacted] to discuss a plan for moving forward.

155. The [redacted] ATO was superseded by an ATO, dated [redacted][lviii] The [redacted] ATO removed KILSWITCH from EKB and replaced it with ATAK. The ATO stated:

- This baseline update improves the functionality/security posture for the EKB-CONFIG [redacted] KILSWITCH application was not meeting capability requirements as configured [redacted]

- The ATAK [redacted] was scanned via the HP Fortify Code Scanner, and the NAVAIR [redacted] validator evaluated and assessed the results as "no concern" to the Navy operating environment as installed on the EKB;" and

- The KILSWITCH Mobile Application is no longer an authorized component of the EKB solution. The PM shall ensure that no devices are deployed for use with this application.

User Feedback

156. We interviewed Navy and Marine Corps [redacted] members, [redacted] regarding their experiences using KILSWITCH. All of them stated that [redacted] their tablets did not have the ability to connect with any other tablet. Some Marine Corps [redacted] stated that they were aware that KILSWITCH was used on personal devices.[lix]

157. Most of the witnesses stated that KILSWITCH was an exceptional product that aided in their mission accomplishment. One witness stated, "It is probably the best invention [redacted]

in the last 20 years. . . .It is unbelievably good and useful."[lx] Another witness rated KILSWITCH as a "9.8" out of a possible 10.[lxi]

[redacted]

158. [redacted]

159. [redacted]

160. [redacted]

161. [redacted]

162. [redacted]

Discussion and Analysis

163. We concluded Allegation One is substantiated. We found that versions of DPSS's KILSWITCH and APASS that have been and are currently used in military operations and training most likely have significant cybersecurity vulnerabilities that have not been effectively mitigated.

164. We found that KILSWITCH/APASS [redacted] The intended uses for KILSWITCH/APASS [redacted] We further found that cybersecurity was not a concern for the developers because they expected that the software would be used only for its intended purpose, [redacted] and would not be used widely in operations. We also found that the developers reasonably expected that [redacted] would be used on a limited number of Government-procured, unconnected tablets which further mitigated cybersecurity concerns. Accordingly, we determined that the

DPSS software development team's performance was not improper or below acceptable standards.

165. We found that Navy and Marine Corps users were favorably impressed by KILSWITCH/APASS functionality and that starting in [redacted] the MCAO issued ATOs for ANTABs that were little more than off-the shelf tablet devices running the Android operating system. Further, the MCAO specifically authorized KILSWITCH with a MCCA to be used pursuant to the ATOs on Government-procured ANTABs.

166. We determined that the ATOs alone for ANTABs were ineffective in mitigating the cybersecurity vulnerabilities of KILSWITCH/APASS [redacted]

- [redacted]
- KILSWITCH/APASS [redacted]
- [redacted]

167. With regard to the THS ATO and MAGTAB ATO, we determined that the evidence establishes that the cybersecurity vulnerabilities appear to be adequately mitigated.

168. We note that regardless of the ATOs, [redacted] are using KILSWITCH/APASS on personally procured devices that do not provide adequate cybersecurity protection.

169. We also determined that KILSWITCH/APASS [redacted] We discuss this use below in the Other Matters section. We determined that evidence indicates that members are using KILSWITCH/APASS on both Government and personally-procured devices. We did not find authority for [redacted] to use KILSWITCH/APASS.

170. We determined that Navy [redacted] used KILSWITCH [redacted] IATT, IATO, and ATO. Each authority limited the number of devices and how the devices were used. We determined that any potential vulnerability was adequately mitigated. We are concerned, however, that PMA-281 did not immediately notify the NAO when it discovered that KILSWITCH [redacted]

171. We determined that, at a minimum, KILSWITCH/APASS [redacted]

Conclusion

172. The allegation that versions of DPSS's KILSWITCH and APASS that have been and are currently used in military operations and training have significant cybersecurity vulnerabilities that have not been effectively mitigated is substantiated.

Recommendations

173. That the Chief of Naval Operations (CNO) and the Commandant of the Marine Corps (CMC) ensure that all personnel are using KILSWITCH/APASS only in ways that are consistent with applicable ATOs and that any non-conforming use ceases.

174. [redacted]

175. [redacted]

Actions Taken

176. DPSS personnel have worked collaboratively with APL and DRUCA personnel to improve the cybersecurity, as well as the [redacted] generally, of KILSWITCH/APASS[redacted]

Actions Planned

177. The following actions are planned:

None.

Personnel Actions Taken

None.

ALLEGATION TWO

That the KILSWITCH/APASS vulnerabilities[redacted] **Substantiated.**

Findings of Fact

178. As a preliminary matter, we note that as discussed above in Allegation One Findings of Fact, when used in accordance with the issued ATOs, KILSWITCH/APASS vulnerabilities are mitigated to varying degrees. This mitigation is attributed to the devices on which KILSWITCH/APASS is loaded, the protection built into the devices, as well as the operating systems on which the devices run. However, there is considerable evidence that KILSWITCH/APASS has been used, and continues to be used, in ways that are not consistent with the ATOs.

179. We are not aware of any assessment that DPSS conducted other than SCA that specifically assessed whether the KILSWITCH/APASS [redacted] We note that such testing is not required for S&T software development [redacted] and, in fact, an adjudicated SCA has never been conducted [redacted] Further, with regard to program of record or production development [redacted] the software is developed as part of a system that includes the operating system of the device, the device on which it was loaded, and the inherent cybersecurity protections of the operating system and device itself. Further, we have no information that KILSWITCH [redacted] has been used in any fashion other than on approved devices in accordance with applicable ATOs.

180. As discussed above in Allegation One, the IV&V conducted for the MAGTAB established that KILSWITCH worked [redacted] Also as discussed above, the Marine Corps Systems Command conducted cyber intrusion testing on THS and the results affirm that the system is not susceptible to intrusion.

181. We discussed above that KILSWITCH/APASS did not work [redacted] Accordingly, even though an ANTAB or personally procured device may be [redacted] KILSWITCH/APASS will not function [redacted]

182. In this section, we address the concern of whether vulnerabilities in KILSWITCH/APASS [redacted] We determined that the consequences [redacted] has not been fully assessed, and therefore, are unknown.

183. In response to an [redacted] request from NAVINSGEN as part of our investigation, Naval Air Warfare Center Weapons Division Cyber (NAWCWD-Cyber) prepared a document, "KILSWITCH Preliminary Assessment," in which NAWCWD-Cyber assessed the cybersecurity risks of KILSWITCH [redacted] NAWCWD-Cyber concluded that when KILSWITCH [redacted] is used on EKB the risk of cyber intrusion and compromise is "LOW." NAWCWD-Cyber stated that cyber security relies on both the application and "its system integrated end state." NAWCWD-Cyber considered the security built into the EKB in reaching its conclusion. NAWCWD-Cyber further stated:

> The application as deployed inside an environment that is properly secured and in compliance with [DoD] Cybersecurity policy and best practices is deemed safe to operate. . . . The application is critically dependent on the security controls/boundary applied to the hosting device and network.

184. NAWCWD-Cyber also addressed the cyber vulnerabilities of using KILSWITCH on a tablet that does not employ security measures. NAWCWD concluded:

> [redacted]

[18] NAWCWD added that it provided its opinion "with MODERATE confidence in this assertion, due to the limited data and time available to conduct this evaluation."

185. NAWCWD-Cyber listed in its assessment the [redacted] and other security mechanisms as examples of appropriate host environment security method.

186. NAWCWD-Cyber listed potential cybersecurity issues that we include as a For Official Use Only attachment to this report.

187. The DPSS Software Technical Lead provided information that highlighted that even when used on unapproved devices, significant user action is required in order for KILSWITCH/APASS to be susceptible [redacted] The DPSS Software Technical Lead listed all the actions that the user would need to take.[lxvi]

188. We provided the DPSS Software Technical Lead's input to Division Director for Navy Cybersecurity, Office of the Chief Engineer, Space and Naval Warfare Systems Command [Division Director for Navy Cybersecurity], and APL. The Division Director for Navy Cybersecurity stated that based on the limited information available he could not make a full evaluation of the KILSWITCH cybersecurity risk.[lxvii] However, he stated:

> I cannot concur with the statements made in the emails you provided. It appears to make some broad assumptions that I have no data to confirm. Based on the limited information, I also cannot quantify what level of risk exists. However, if the software has significant vulnerabilities, then running that software on unapproved devices [redacted] most likely does increase the risk of the device and software being exploited. I cannot quantify the level of risk with the data I was provided.

189. APL responded to our request for comment by stating:[lxviii]

> [redacted] However, it does not mean that users won't choose to do something they should not do, even if it violates policy; particularly if the user sees it as necessary to achieve a mission.

190. Of significant importance, APL further stated:

> [redacted] KILSWITCH itself (e.g., other apps on the device, Wi-Fi/Bluetooth connections, vulnerable OS).

Discussion and Analysis

191. We determined that the vulnerabilities in KILSWITCH/APASS [redacted] We are unable to quantify those risks.

Conclusion

192. The allegation that the KILSWITCH/APASS vulnerabilities [redacted] is substantiated.

Recommendations

193. That KILSWITCH/APASS be used only on devices that provide adequate host environment security methods.

Actions Taken

194. None.

Actions Planned

195. None.

Personnel Actions Taken

196. None.

OTHER MATTERS

197. We determined that APASS is being used extensively by [redacted] We also discovered information that indicated that NAWCWD personnel were "marketing" KILSWITCH/APASS to potential users, including [redacted]

198. In response to written questions from us, the [redacted] provided a consolidated written response regarding how APASS is being used [redacted] The response established that APASS has been used by [redacted] Further, the response acknowledges that [redacted] authority to use APASS.

199. With regard to use by [redacted] stated that [redacted] used and continue to use APASS extensively. [redacted] KILSWITCH/APASS [redacted] [redacted] He stated that the application was first used by [redacted] [redacted] He stated that the [redacted] [redacted] made APASS available. [redacted] that APASS has been loaded onto over 400 Government-procured commercial off-the-shelf devices. Each of these devices has wireless, cellular, Bluetooth, and GPS functionality.[lxxi]

200. Regarding authority to use APASS, [redacted] stated, "there was no ATO that specifically said you could or you could not use it."[lxxii] He added, however, that [redacted] use of APASS "was briefed through our chain of command all

the way up [redacted][lxxiii] He also added that APASS was used only as a planning tool and for situational awareness and never used operationally "because it's not authorized."[lxxiv]

201. Regarding whether APASS use by [redacted] stated that its use is "everywhere . . . . It's widely used" and being used by [redacted] stationed on the [redacted] He added that he believes it is not limited to [redacted] but also used by other services.

202. [redacted] response also established that [redacted] used APASS since [redacted], when it was released for use by [redacted]. [redacted] stated that APASS was used only by [redacted] He stated that APASS use is now limited by [redacted] because [redacted] has selected ATAK as the app for [redacted] He also stated that for a period approximately from [redacted] tablets that were used in operations were personally procured [redacted]

203. [redacted] stated that when he arrived at his assignment, [redacted] were using both APASS and ATAK in training and operations.[lxxv] He estimated that the number of users for each app was about the same and added that APASS was loaded onto Government-issued tablets as well as personal Android phones.[lxxvi]

204. [redacted] said he was concerned about personnel using APASS because he knew the Complainant and was aware of this complaint [redacted] He also stated that there was no authority to use APASS.[lxxvii] He said that he directed users to not use APASS but to use ATAK.

205. We recommend that [redacted] determine whether APASS is authorized for use by [redacted] on approved devices, and if not, ensure that such use ends. We further recommend that [redacted] prohibit the use of APASS on personally procured devices.

KILSWITCH/APASS Marketing

206. As discussed above, the [redacted] sent an e-mail that had attached a presentation, "KILSWITCH: Combat Proven by Marines since [redacted]"[lxxviii]

207. We also discussed above that DRUCA issued a "Static Analysis Certification," dated [redacted] for KILSWITCH [redacted] [redacted] This certificate stated that KILSWITCH [redacted] defects using Fortify and Klocwork SCA tools. This was the first certificate that DRUCA issued. We note that it was issued within one month of when [redacted] were informed of the 1,277 page [redacted] SCA Report. We discovered that this certificate was distributed to KILSWITCH/APASS users and others to counter concerns with KILSWITCH that arose based on the [redacted] SCA report.

208. We also reviewed an e-mail, dated [redacted] that the Director, Software and Mission Systems Integration Department, NAWCWD, (Director, Software and Mission Systems) sent with the subject: "APASS Suitability," [redacted][lxxx] The Executive Director and Director for Research and Engineering, NAWCWD (Executive

Director), is cc'ed on this message. In the e-mail the Director, Software and Mission Systems wrote, in part:

> KS [KILSWITCH]/APASS is safe for combat operations.
>
> The following measures have been taken to ensure that KS/APASS continues to be safe and suitable for combat operations. Independent verification has been done by the Marine Corps on the software baseline and they have issued multiple ATOs indicating their confidence in the software as well. ATOs including the KS/APASS application are the MAGTAB ATO, THS ATO, and EKB ATO. These three ATOs cover the application in different combinations of hardware configurations and network connectivity.
>
> The DPSS team in collaboration with the DRUCA Software Assurance team at NAWCWD has initiated regular interval software scans with several different Static Code Analysis scanning tools called HP Fortify and Klocwork. The scans allow the DRUCA team to analyze the tools identified "potential" vulnerabilities and adjudicate the results with the DPSS team which may result in [redacted] We say potential vulnerabilities because not all findings within the scan tool are actual problems. 100% of adjudicated PRI 1 and PRI 2 defects are mandatorily corrected prior to any software release. Software change modifications are tracked under configuration management to ensure product integrity. PRI 3 defects are boarded and addressed under DPSS's Software Configuration Review Board and addressed for correction. All remaining adjudicated defects are dispositioned and reported to provide a complete review of all findings.
>
> . . .
>
> Specifically in the case of combat operations and the [redacted] the independent assessment done by the Marine Corps cyber security in support of the THS program determined that the risk was extremely small and signed a full risk acceptance letter after the initial review.

209. [redacted] forwarded the e-mail to 14 recipients with [redacted] e-mail addresses and 10 other recipients, not including the Director, Software and Mission Systems and Executive Director who remained as cc's on the e-mail. We noted that this e-mail was sent within 2 weeks of when [redacted] were informed of the 1,277-page [redacted] SCA Report.

210. We found that the e-mail was inaccurate, incomplete, and misleading in various respects, including:

- USMC had not conducted independent verification (IV&V) of any version of the KILSWITCH/APASS[redacted]

- DRUCA conducted adjudicated SCA of KILSWITCH/APASS [redacted] THS (THS [redacted]
- DRUCA did not conduct an adjudicated SCA of KILSWITCH/APASS [redacted]
- At the time of the e-mail, the Marine Corps Systems Command had not conducted an assessment [redacted] KILSWITCH/APASS software at the USMC cyber range; and
- The assessment by the Marine Corps Systems Command at the USMC cyber range was of the THS device and not the KILSWITCH/APASS software.

211. We are further troubled that the Director included in his e-mail references to ATOs that did not apply to [redacted] yet acknowledged that KILSWITCH/APASS were being used in combat operations.

Appendix A – Reference Documents

1. Document 1-OSC Tasker DI-17-3391
2. Document 2-[redacted]e-mail
3. Document 3-[redacted] e-mail Atch KILSWITCH-APASS brief for ACMC
4. Document 4-DRUCA Data e-mail
5. Document 5-DRUCA Data e-mail Atch
6. Document 6-DRUCA Static Analysis Cert
7. Document 7- [redacted]
8. Document 8-[redacted] SCA Report
9. Document 9-[redacted] EKB-PROG
10. Document 10-APL [redacted] Rpt
11. Document 11-APL [redacted] Rpt
12. Document 12-SARA Lab Rpt
13. Document 13-APL [redacted] Rpt
14. Document 14-APL Response [redacted]
15. Document 15-APL Response [redacted]
16. Document 16-[redacted]
17. Document 17-ANTAB ATO State 0
18. Document 18-ANTAB ATO State 1 - [redacted]
19. Document 19-ANTAB ATO State 1 - [redacted]
20. Document 20-MCCA KILSWITCH
21. Document 21-THS ATO
22. Document 22-MAGTAB ATO
23. Document 23-MAGTAB_SAR_IV&V
24. Document 24-IATT-KILSWITCH
25. Document 25-IATO-KILSWITCH
26. Document 26-EKB ATO [redacted]
27. Document 27-EKB ATO [redacted]
28. Document 28-[redacted]
29. Document 29-[redacted]
30. Document 30-NAWCWD KILSWITCH PA
31. Document 31-[redacted]
32. Document 32-[redacted]
33. Document 33-[redacted]
34. Document 34-[redacted]
35. Document 35-APL re Security
36. Document 36-[redacted] e-mail

Appendix B – Witness List

1. The Complainant, by telephone

[redacted]

[redacted]

Appendix C – Consolidated List of Recommendations

Allegation One Recommendations

1. That the Chief of Naval Operations (CNO) and the Commandant of the Marine Corps (CMC) ensure that all personnel are using KILSWITCH/APASS only in ways that are consistent with applicable ATOs and that any non-conforming use ceases.

2. That the CNO and the CMC take appropriate action [redacted]

3. That the CNO and the CMC ensure that KILSWITCH/APASS [redacted]

Allegation Two Recommendations

1. That KILSWITCH/APASS be used only on devices that provide adequate host environment security methods.

Appendix D – Acronym List

AFRL - Air Force Research Laboratory, Rome Labs
ANTAB - Android Tablet
APASS - Android Precision Assault Strike Suite (software application)
APL - Applied Physics Lab
ATAK - Android Tactical Assault Kit
ATO - Authority to Operate
CAC - Common Access Card
CONOPS - Concept of Operations
[redacted]
DARPA - Defense Advanced Research Projects Agency
DPSS - Digital Precision Strike Suite
DPSS DPM - DPSS Deputy Program Manager
DRUCA - Naval Air Systems Command Defect Reduction Using Code Analysis
EKB - Electronic Kneeboard
[redacted]
FFRDC - Federally Funded Research and Development Center
IA - Information Assurance
IATO - Interim Authorization To Operate
IATT - Interim Authorization To Test
IO - Investigating Officer
IV&V - Independent Verification & Validation
JTAC -Joint Terminal Attack Controller
KILSWITCH - Kinetic Integrated Low-Cost Software Integrated Tactical Combat Handheld (software application)
MAGTAB - Marine Air Ground Tablet
MAWTS-1 - Marine Corps Aviation Weapons and Tactics Squadron One
MCAO - Marine Corps Approving Official
MCCA - Marine Corps Certified Application
MCCAST - Marine Corps Certification and Accreditation Tool
NAVAIR - Naval Air Systems Command
NAVINSGEN - Office of the Naval Inspector General
NAWCWD - Naval Air Warfare Center Weapons Division
NAWCWD-Cyber - Naval Air Warfare Center Weapons Division - Cyber
NSW - Naval Special Warfare
PCAS - Persistent Close Air Support
PMA-281 - Program Management Activity-281
[redacted]
SARA - Software Assurance Research & Applications Lab
SCA - Static Code Analysis
SECDEF - Secretary of Defense
SEI - Software Engineering Institute
SECNAV - Secretary of the Navy
[redacted]

STIG - DoD Security Technical Implementation Guide
THS - Target Hand-Off System
UARC - University-Affiliated Research Center Laboratory
[redacted]
USMC - United States Marine Corps

[i] Document 1.
[ii] Document 2 and 3.
[redacted]
[ix] Document 4 and 5.
[x] Document 6.
[xi] Document 7, p. 11.
[xii] Document 7, p. 10.
[xiii] Document 7, p. 10.
[xiv] Document 7, p. 9.
[xv] Document 8.
[xvi] Document 7, p. 5.
[xvii] Document 9.
[xviii] Document 10.
[xix] Document 11.
[xx] Document 12.
[xxi] Document 13.
[xxii] Document 14.
[xxiii] Document 15.
[redacted]
[xxxix] Doc 16.
[redacted]
[xli] Document 17.
[xlii] Document 18.
[redacted]
[xlv] Document 19.
[redacted]
[xlvii] Document 20.
[redacted]
[xlix] Document 21.
[l] Document 22.
[li] Document 23.

[lii] Document 24.

[redacted]

[lv] Document 25.

[lvi] Document 26.

[lvii] Document 7.

[lviii] Document 27.

[lix] Confidential witness, p. 10.

[redacted]

[lxii] Document 28.

[lxiii] Document 29.

[redacted]

[lxv] Document 30.

[lxvi] Documents 31, 32, and 33.

[lxvii] Document 34.

[lxviii] Document 35.

[redacted]

[lxxviii] Documents 2 and 3.

[lxxix] Document 6.

[lxxx] Document 36.