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

The Special Counsel

October 22, 2014

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

Re: OSC File No. DI-13-3640

Dear Mr. President:

Pursuant to my duties as Special Counsel, enclosed please find the U.S. Department of the Navy's (Navy) investigative report based on disclosures of wrongdoing at the Space and Naval Warfare Systems Command (SPAWAR) Systems Center Pacific made to the U.S. Office of Special Counsel (OSC). OSC has reviewed the report and, in accordance with 5 U.S.C. § 1213(e), provides the following summary of the allegations and our findings.

The whistleblower, David Richardson, disclosed to OSC that SPAWAR Systems Center Pacific employees and contractors engaged in conduct that created a substantial and specific danger to Navy personnel and the general public. Specifically, Mr. Richardson alleged that SPAWAR Systems Center Pacific used a method of monitoring cyber warfare threats that interfered with command communications within the Fleet Area Control and Surveillance Facility San Diego (FACSFAC) and the Southern California Offshore Range (SCORE). He disclosed that this interference resulted in a complete shutdown of both visual and auditory communication between range participants and SCORE's Range Operations Center (Operations Center).[1] On September 27, 2013, OSC referred these allegations to Secretary of the Navy Ray Mabus to conduct an investigation pursuant to 5 U.S.C. § 1213(c) and (d).

The Navy did not substantiate Mr. Richardson's allegations that the Commander, U.S. Pacific Fleet's (COMPACFLT) means of conducting information assurance activities caused regular disruption to command communications within SCORE, or that the lives of Navy personnel and the general public were endangered. The agency concluded that no loss of communication could be attributed to information assurance measures. Further, the report concluded that there are safety procedures that prevent any loss of communication or outage from causing a safety hazard on SCORE-controlled ranges. Notwithstanding the findings, the agency took action to improve communications. Based on my review, I have determined that the report meets all statutory requirements and that the findings appear to be reasonable.

---

[1] Early in its investigation, the Navy discovered that the Information Assurance Division of the Communications and Information Systems Directorate on the Staff of the Commander, Pacific Fleet, rather than SPAWAR Systems Center Pacific, is responsible for the alleged activities. Mr. Richardson concurred with this finding.

After receiving OSC's referral, Secretary Mabus tasked the COMPACFLT Inspector General with conducting an investigation of Mr. Richardson's allegations. On February 18, 2014, Secretary Mabus submitted the agency's report to OSC. Pursuant to 5 U.S.C. § 1213(e)(1), Mr. Richardson was given the opportunity to review and comment on the agency report and declined to do so on April 8, 2014. As required by 5 U.S.C. § 1213(e)(3), I am now transmitting the report to you.[2]

According to Mr. Richardson, SCORE contains an embedded network of wiring, connecting twenty-seven major units of the Pacific Fleet, including radar, hydrophones, threat emitters, live target simulators, and communication systems. Mr. Richardson alleged that COMPACFLT conducts information assurance activities, including cyber warfare and countermeasures, in a manner that disrupts SCORE's network and interferes with the Operations Center's ability to monitor, control, evaluate, and maintain communication with SCORE's range during live fire tactical training exercises. Mr. Richardson alleged that disruption of both auditory and visual communication between range participants and Operations Center personnel occurs when COMPACFLT personnel force connections of the internal SCORE wiring which is incompatible with the Navy-Marine Corps Intranet (NMCI). NMCI is the Navy's internal integrated network and operates separately from SCORE. Mr. Richardson asserted that these communication blackouts occur at least once a day and disable radio voice communications between Operations Center personnel and participating combat ships, submarines, and aircraft.

The agency report concluded that communication disruptions occur infrequently and, when they do occur, are not attributed to COMPACFLT's information assurance activities. Further, the investigation revealed that SCORE employs two communication channels and has procedures in place to prevent these instances from causing a safety hazard. Regarding the allegations of unplanned outages, the report indicated that SCORE schedules maintenance periods for its computer network, about which Mr. Richardson was unaware prior to making his disclosures. Investigators interviewed witnesses who confirmed that these maintenance periods are scheduled in advance and have no impact on exercises in SCORE-controlled ranges.

---

[2] The U.S. Office of Special Counsel (OSC) is authorized by law to receive disclosures of information from federal employees alleging violations of law, rule, or regulation, gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health and safety. 5 U.S.C. § 1213(a) , (b). OSC does not have the authority to investigate a whistleblower's disclosure; rather, if the Special Counsel determines that there is a substantial likelihood that one of the aforementioned conditions exists, she is required to advise the appropriate agency head of her determination, and the agency head is required to conduct an investigation of the allegations and submit a written report. 5 U.S.C. § 1213(c).

Upon receipt, the Special Counsel reviews the agency report to determine whether it contains all of the information required by statute and that the findings of the head of the agency appear to be reasonable. 5 U.S.C. § 1213(e)(2). The Special Counsel will determine that the agency's investigative findings and conclusions appear reasonable if they are credible, consistent, and complete based upon the facts in the disclosure, the agency report, and the comments offered by the whistleblower under 5 U.S.C. § 1213(e)(1).

Notwithstanding these findings, the report identified an underlying security concern related to information assurance requirements that impacts SCORE's ability to respond to various threats. Because SCORE uses a commercial internet service provider, weakness in security has been a concern since 2010. Thus, FACSFAC and CAMPACFLT have taken steps to operate the SCORE computer network more securely. Since 2010, FACSFAC and CAMPACFLT have progressed towards converting the SCORE network to the NMCI. Further, prior to August 2013, SCORE did not maintain communication with units conducting ground exercises on the in-shore and near-shore San Clemente Island ranges, and relied on scheduling to ensure the safety in these areas. Accordingly, SCORE established a Range Coordination Center on August 19, 2013, to conduct ground exercises more efficiently and securely. According to the report, when interviewed, Mr. Richardson agreed that since these measures have been taken, his safety concerns have been adequately addressed.

As required by 5 U.S.C. § 1213(e)(3), I have sent copies of the unredacted agency report to the Chairmen and Ranking Members of the Senate and House Committees on Armed Services. The redacted report identifies Navy employees and witnesses by title only and contains certain language substituted to maintain the confidentiality of the parties involved. [3] I have also filed copies of the redacted report in our public file, which is available online at www.osc.gov. This matter is now closed.

Respectfully,

Carolyn N. Lerner

Enclosures

[3] The Navy provided OSC with a redacted report, which substituted titles for the names of Navy employees and other individuals referenced therein. The Navy cited the Freedom of Information Act (FOIA) (5 U.S.C. § 552) and the Privacy Act of 1974 (Privacy Act) (5 U.S.C. § 552a) as the basis for these revisions to the report produced in response to 5 U.S.C. § 1213. OSC objects to the Navy's use of the FOIA and Privacy Act to remove the names of these individuals on the basis that the application of the FOIA and Privacy Act in this manner is overly broad.