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

The Special Counsel

December 1, 2015

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

Re: OSC File Nos. DI-13-2309 and DI-13-2348
Dear Mr. President:

Pursuant to my duties as Special Counsel, enclosed please find agency reports based on disclosures of wrongdoing at the Department of the Navy, (Navy), Strategic Systems Programs (SSP), Washington Navy Yard, D.C. The Office of Special Counsel (OSC) has reviewed the reports, and, in accordance with 5 U.S.C. § 1213(e), provides the following summary of the agency report, whistleblower comments, and my findings.

The whistleblowers, former Echelon II Command Security Manager Sparky Edwards and former Deputy Security Manager Vernon Londagin, who consented to the release of their names, disclosed that SSP employees engaged in conduct that may constitute a violation of law, rule or regulation; gross mismanagement; and a substantial and specific danger to public safety by failing to resolve numerous security deficiencies within SSP headquarters and other security vulnerabilities at the Washington Navy Yard.

The Naval Inspector General (IG) conducted the investigation and substantiated all but one of the primary allegations of security deficiencies and violations. The report confirmed that the physical and information security deficiencies violated Department of Defense (DoD) and Navy regulations, directives, instructions, and rules. In response to the findings, the agency completed all of the recommended corrective actions, including a comprehensive security-in-depth review of SSP headquarters to confirm the effectiveness of SSP's security program. I have reviewed the original disclosures, the agency reports, and whistleblowers' comments. I have determined that the reports meet all statutory requirements and that the agency's findings appear reasonable.

The whistleblowers' allegations were referred to then-Secretary of Defense Chuck Hagel on September 25, 2013, to conduct an investigation pursuant to 5 U.S.C. § 1213(c). Secretary Hagel authorized Secretary of the Navy Ray Mabus to investigate the allegations and submit the report to OSC. Secretary Mabus directed the Naval IG to conduct the investigation. The agency submitted its report to OSC on August 15, 2014, and a supplemental report on June 1, 2015. The whistleblowers provided comments on the reports

pursuant to § 1213(e)(1). As required by 5 U.S.C. § 1213(e)(3), I am now transmitting the reports and whistleblower comments to you.[1]

SSP, with headquarters located in Building 200 of the Navy Yard, is responsible for the Navy's Fleet Ballistic Missile Strategic Weapons System. Much of the information SSP maintains is classified as national security information. The whistleblowers alleged that between May 2012 and March 2013, they identified numerous deficiencies and violations of security requirements at SSP and the Washington Navy Yard. Despite the sensitive nature of SSP's work, as well as public access and lenient entry procedures to the Washington Navy Yard, Building 200 did not have a security guard and was left unlocked 24 hours per day. The whistleblowers further reported that SSP's Controlled Access Areas and Open Storage Secret Areas, where classified information is maintained, were not properly certified and did not have the required security features to protect against intrusion. Among other issues, the whistleblowers observed that the Secret Internet Protocol Router Network (SIPRNet) used for classified information was not properly protected, and employees left SIPRNet terminals logged-in to the network with computer screens facing open windows. The whistleblowers reported these deficiencies to SSP leadership and asserted that appropriate action was not taken to resolve the problems.

The investigation substantiated that: (1) the procedures for entry to the Washington Navy Yard permitted access to people who were not properly screened;[2] (2) SSP Controlled Access Areas and Open Storage Secret Areas did not meet physical and information security requirements and were improperly certified; (3) SSP's SIPRNet was not secure because of the deficiencies in the Controlled Access Areas and Open Storage Secret Areas; (4) employees stored and used cellular phones and other personal electronic devices in those areas, which is prohibited; (5) SSP safes used for storing classified material were not properly inspected or updated with new combinations as required; (6) employees left Common Access Cards unattended in workstations, and in at least one instance, positioned a computer screen displaying classified information toward an uncovered window. The report confirmed that these physical and information security deficiencies violated DoD and Navy regulations, directives, instructions, and rules. In addition, the investigation confirmed that the whistleblowers had communicated valid security concerns to SSP management, with no definitive action taken in response. The report concluded that the SSP director did not meet

---

[1]The Office of Special Counsel (OSC) is authorized by law to receive disclosure of information from federal employees alleging violation 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) and (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 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) and (g). 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).

[2]For this allegation, the Naval IG relied on the conclusions of the November 2013 Judge Advocate General Manual (JAGMAN) investigation of the fatal shooting incident at the Washington Navy Yard on September 16, 2013. Corrective actions were taken pursuant to the recommendations contained in the JAGMAN report.

his responsibility to ensure that all physical and information security standards were met to safeguard classified material. Nevertheless, the investigation found no evidence of loss or actual compromise of classified material.

In response to these findings, the agency implemented all of the corrective actions that the Naval IG recommended, and the reports confirmed that all of the security deficiencies identified within SSP headquarters have been corrected. Further, the agency completed the additional tasks that Secretary Mabus directed, including a comprehensive security-in-depth review of SSP. That review confirmed that SSP had an overall effective security program with a few exceptions that were being addressed through additional corrective actions, including changes in policy and organizational structure. The SSP director received an administrative counseling for failing to meet his oversight responsibilities following an accountability review by the vice chief of Naval Operations.

The whistleblowers provided comments on the agency reports, which are enclosed. Their comments clarified, and in some instances refuted, the factual findings in the reports. The whistleblowers also raised concerns regarding the objectivity of the security-in-depth review in light of the longstanding relationships between the involved Navy and SSP officials.

I have reviewed the original disclosures, agency reports, and whistleblower comments. While I recognize the whistleblowers' concerns, I have determined that the reports contain all of the information required by statute and that the findings appear to be reasonable. As required by 5 U.S.C. § 1213(e)(3), I have sent copies of the unredacted agency reports and whistleblower comments to the Chairmen and Ranking Members of the Senate Committee on Armed Services and the House Armed Services Committee. I have also filed copies of the redacted agency reports and whistleblower comments in our public file, which is available online at www.osc.gov.[3] OSC has now closed this file.

Sincerely,

Carolyn N. Lerner

Enclosures

[3]The agency provided OSC with an unredacted report (enclosed) that is marked For Official Use Only and contains privacy sensitive information and information protected under agreement between the United States and United Kingdom. The agency also provided a redacted report for public release removing the privacy sensitive and protected information. OSC concurs with these redactions. The agency also redacted employee names from the version for public release, citing 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 agency'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.