



U.S. Office of Special Counsel
1730 M Street, N.W., Suite 218
Washington, D.C. 20036-4505

Whistleblower Disclosures of Security Vulnerabilities at the Navy Yard are Confirmed

FOR IMMEDIATE RELEASE

CONTACT: Nick Schwellenbach, (202) 254-3631; nschwellenbach@osc.gov

WASHINGTON, D.C./December 2, 2015 –

The U.S. Office of Special Counsel (OSC) [informed](#) the White House and Congress yesterday that the Navy substantiated numerous whistleblower disclosures at the Washington Navy Yard, particularly information security vulnerabilities at the Strategic Systems Programs (SSP), headquartered in Building 200 (the 2013 shooting occurred on the other side of the Navy Yard in Building 197). The whistleblowers were former Echelon II Command Security Manager Sparky Edwards and former Deputy Security Manager Vernon Londagin. SSP is responsible for the Navy's Fleet Ballistic Missile Strategic Weapons System. Much of the information maintained by SSP is highly classified.

Mr. Edwards and Mr. Londagin initially blew the whistle internally at the Navy in 2012 and 2013. They subsequently turned to OSC because they did not believe that SSP leadership took adequate steps to address the problems. OSC compelled the Navy to fully investigate their disclosures.

The Naval Inspector General's (Naval IG) [investigation](#) substantiated that during the time frame alleged: (1) the procedures for entry to the Washington Navy Yard permitted access to people who were not properly screened (note: the Navy addressed the problems with these procedures following another, earlier Navy [investigation](#) in the immediate wake of the 2013 shooting); (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 network for exchanging classified information was not secure because of 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; and (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.

In addition, the investigation confirmed that the whistleblowers had communicated valid security concerns to SSP management, which took no definitive action in response. The report concluded that the SSP director did not meet his responsibility to ensure that all physical and information security standards were met to safeguard classified material. However, the investigation found no evidence of loss or actual compromise of classified material.

The vice chief of Naval Operations conducted a follow-up accountability [review](#) in 2015, which led to an administrative counseling of the SSP director.

The Naval IG has confirmed that all security deficiencies identified have been corrected.

"I want to thank Mr. Edwards and Mr. Londagin, whose disclosures have improved the security of our nation's classified information," said Special Counsel Carolyn Lerner.

The U.S. Office of Special Counsel (OSC) is an independent federal investigative and prosecutorial agency. Our basic authorities come from four federal statutes: the Civil Service Reform Act, the Whistleblower Protection Act, the Hatch Act, and the Uniformed Services Employment & Reemployment Rights Act (USERRA). OSC's primary mission is to safeguard the merit system by protecting federal employees and applicants from prohibited personnel practices, especially reprisal for whistleblowing, and to serve as a safe channel for allegations of wrongdoing. For more information, please visit our website at www.osc.gov.