

Altmire, Casey Press for Answers on Marine One Security Breach

(WASHINGTON, D.C.) -- U.S. Congressman Jason Altmire (PA-04) and U.S. Senator Bob Casey (D-PA) announced today that they have sent a letter to the Under Secretary of Defense for Acquisition, Technology and Logistics John J. Young, Jr. asking for additional information on the recent security breach regarding the Presidential helicopter, Marine One.

(WASHINGTON, D.C.) -- U.S. Congressman Jason Altmire (PA-04) and U.S. Senator Bob Casey (D-PA) announced today that they have sent a letter to the Under Secretary of Defense for Acquisition, Technology and Logistics John J. Young, Jr. asking for additional information on the recent security breach regarding the Presidential helicopter, Marine One. Specifically, Altmire and Casey asked when and by whom this security breach was discovered, the nature of the information compromised, and what corrective actions the Navy is taking to prevent similar incidents from occurring in the future.

"I want to make sure that our armed forces and defense contractors are taking every precaution necessary to ensure that sensitive information is absolutely secure," Altmire said. "In an age when hostile foreign governments are constantly searching the internet to find information that can compromise our security, we need to make sure that our government is being as vigilant as possible."

"This apparent security breach involves two emerging challenges to U.S. national security: Iran's pursuit of regional hegemony in the Middle East and the growing threat to our nation's cyber security," said Senator Casey. "I strongly urge the Pentagon to closely look into this matter and take the necessary steps to ensure our sensitive technology is not compromised by foreign adversaries."

In February, Tiversa -- a company based in Cranberry, PA -- discovered that engineering and communications documents containing key details about the Marine One fleet had been downloaded to an IP address in Iran. The documents were traced back to a defense contractor in Maryland, where an employee most likely downloaded a file-sharing program which inadvertently allowed others to access this information on his or her hard drive.

Recent reports have said that the federal government was warned last June that an internet website with an IP address traced to Iran was actively seeking this information. Although a review by the Department of the Navy found that the release of these documents posed no significant threat to the presidential helicopter program, the ease with which these files could be accessed highlights a potentially damaging vulnerability in our nation's defense system.