United States Senate
WASHINGTON, DC 20510

March 12, 2015

U.S. Department of State
Office of Inspector General
Room 8100, SA-3
2201 C Street, N.W.
Washington, DC 20520-0308

Dear Inspector General Linick:

We write to you today concerning the recent revelations that former Secretary of State Hillary Clinton and other top aides used non-State Department email addresses and servers to conduct official U.S. Government business. We are concerned that diplomatically sensitive, and possibly classified, information may have been transmitted and stored in an insecure manner.

Foreign intelligence organizations and malicious actors continuously probe our government's information systems for weaknesses and attempt targeted intrusions. As you know, the federal government has experienced a number of sophisticated intrusions in recent years, and the threat is only growing. The use of privately maintained information systems that are not protected by federal government experts and key technical capabilities raises serious concerns as those networks may be less secure. Moreover, if a non-government server was known to be a repository for the Secretary's emails, it would almost certainly become—if it is not already—a priority target for foreign intelligence services and others.

To ensure appropriate security protections for sensitive but unclassified information the State Department's Foreign Affairs Manual policy, in place since 2005, requires that "normal day-to-day operations be conducted on an authorized AIS [Automated Information System], which has the proper level of security control to provide nonrepudiation, authentication and encryption, to ensure confidentiality, integrity, and availability of the resident information." The policy also states that "employees are expected to use approved secure methods to transmit SBU [sensitive but unclassified] information when available and practical." Furthermore, it is our understanding that the State Department has specifically instructed its employees, ostensibly during Secretary Clinton's tenure, to avoid conducting official Department business from personal e-mail accounts.

In addition, there are serious questions about the use of such non-government accounts on federal recordkeeping and transparency, particularly if it results in non-compliance with the Federal Records Act and National Archives and Records Administration (NARA)

regulations. Potential noncompliance with these requirements, many of which are imposed by federal law, is a serious matter.

We ask that your office, in coordination with the Inspector General for the Intelligence Community, and any other appropriate Federal entities, conduct a thorough audit related to electronic communications by State Department employees, including former senior officials, that were principally carried out on non-government-owned, or non-government-protected, information networks. Further, we ask that you provide a written report to the relevant congressional committees detailing your findings and any recommendations. The report should include the following:

1. The names and positions of State Department officials who regularly used non-official email to conduct official government business.

2. A specific description of the non-government information networks or systems that were used to transmit such email, to include:
    a. the network security measures in place on such networks and systems from 2009 to 2013;
    b. the means, if any, by which the network's security incorporated classified cyber security threat information controlled by the U.S. government;
    c. the type of wireless communication devices that connected to the systems;
    d. the location and ownership of the servers and other components of such networks or systems;
    e. the names of individuals and entities that had authorized access to such networks or systems, including specifically those with authorized administrative access; and
    f. the funding source for the system, its maintenance, upkeep, and administration.

3. An assessment of whether any of the State Department or other U.S. or foreign government information transmitted or received on such networks or systems contained classified, sensitive but unclassified, diplomatically sensitive, or otherwise nonpublic material.

4. A determination of whether any non-government emails used to conduct official government business or other government information has been deleted from these information networks or systems or altered from their original content, and, if applicable, an estimate of the number of emails or material that was deleted or altered.

5. A determination of whether all emails and other information that was required to be archived pursuant to the Federal Records Act or other legal or regulatory requirements were provided to the State Department or other government agencies for archiving, and whether the timing and nature of these actions was consistent with State Department policy, as well as applicable federal law and regulations.

We ask that this be an unclassified report, and that a classified annex be provided if necessary. Thank you for your time, and we look forward to working with you on this important matter of national security.

Sincerely,

Chairman Bob Corker
Senate Foreign Relations Committee

Chairman Richard Burr
Senate Select Committee on Intelligence

Chairman Ron Johnson
Senate Homeland Security and
Governmental Affairs Committee