EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF ADMINISTRATION
WASHINGTON, D.C. 20503

January 15, 2010

Meredith Fuchs
Counsel for National Security Archive
George Washington University
2130 H Street, NW
Gelman Suite 701
Washington, D.C. 20037

Anne Weismann
Counsel for CREW
Citizens for Responsibility and Ethics in Washington
1400 Eye Street, N.W., Suite 450
Washington, D.C. 20005

Dear Ms. Fuchs and Ms. Weismann:

As part of our ongoing commitment to preserve White House records and promote government accountability, we are providing you with a description of our current system for preserving and archiving unclassified White House emails.

Since January 20, 2009, the Executive Office of the President (EOP) has relied on EMC Corporation's EmailXtender (EX) as its electronic mail storage system for the EOP's unclassified network. This system was selected because it:

- Is a secure, single, centrally managed email archive with EOP component based repositories;
- Automatically captures messages from Microsoft Exchange Journal Servers, including messages sent or received via Blackberries, in near real-time;
- Supports Microsoft Exchange 2000 (the existing email system) and 2007 (which will be deployed in FY10);
- Archives Messages in original format with attachments;
- Facilitates the frequent backups on disaster recovery tapes that EOP conducts according to industry best practices:
- Full, automated backup done the second Tuesday of each month; and
    - Incremental backups performed every Monday, Wednesday, Friday, and Sunday;
- Provides a searchable on-line archive with access controls and audit reporting;
- Provides weekly automated audit reports;
- Includes system health-check dashboard reports which are monitored 24 x 7 by Network Operations Staff;

- Provides email de-duplication and compression, reducing storage requirements;
- Can segregate emails by component and therefore differentiates between PRA and FRA entities; and
- Can be extracted into .eml format for transfer to the National Archives and Records Administration's Electronic Records Archive system

Emails sent or received in the EOP unclassified network are bifurcated so that identical copies of each message are sent to the appropriate user-controlled mailboxes and, through the Exchange Journal servers to the EX Archive servers. EX automatically captures email from the Exchange Journal servers in near real-time. Because EX is able to identify the relevant component(s) for each message, EOP can differentiate between PRA and FRA records.

As in most IT environments, the use of handheld devices has become very prevalent across the EOP. Our messaging environment includes Research In Motions' Blackberry devices. Email messages sent or received via Blackberry devices flow through the journal servers and are captured in the EX system in the same manner as emails sent or received via the desktop.

Staff does not have the ability to access personal email accounts though the EOP network because the EOP network blocks all known web based external email systems. Neither the EOP network nor EOP Blackberry devices permit the use of known instant messaging services.

The EX system offers broad search capabilities. The search capacity of EX is user-friendly. A simple keyword can yield relevant results and searches can be performed according to the sender and/or recipient. EX is also capable of utilizing Boolean logic. These capabilities are, however, limited as to who can use them, and what they can do. Searches are "read" only. There is no way to alter, edit, change or delete an email. Moreover, EOP has designated only certain individuals per component with the authority to conduct searches on EX. Typically the components have delegated this ability to staff in their General Counsel's Office or Records Management team who, after being trained on the search function, can search only their component's email repositories.

EOP routinely monitors EX. Dashboard reports are created and are carefully monitored by the EOP's network operations center 24 x 7 to ensure system functionality. Dashboard reports detail the capacity of the network and confirm remaining email storage capacity.

In addition to the dashboard reports, weekly audit reports are automatically generated and sent to EOP's Records Management team. They detail any searches performed across all repositories, identifying the name of the individual who ran the search and if the individual opened any email messages resulting from the search. These audit reports verify that only authorized individuals accessed the repositories. Moreover authorized access is limited to read-only search results.

It is not possible for an individual to remove any messages stored within the EX system without detection. Another automated weekly audit report details any message which has been removed from any repository.

There is a need, though rare, to remove messages from the system when data spills occur. A data spill is when an EOP user sends or receives data containing classified material. When this

occurs, the Information Security team is engaged. Information Security determines the containment strategy and seeks the approvals of OCIO management to proceed. When the appropriate approvals have been given, the security team directs the EX system administrators to remove the classified data from the system repository(s). The EX system administrators are the only personnel who have the ability to remove data from the EX system, and cannot delete messages without advice from the Office of Security and Emergency Preparedness, the National Security Council, and the authorization of the Chief Information Officer, the Office of General Counsel, and the Director of OA. The unique Microsoft message ID number is used to ensure that the EX system administrators remove only the specific targeted data. The Records Management team confirms, via the weekly audit reports, that only the targeted messages have been removed. A record copy of all such targeted messages is preserved. Each data spill event is documented to include a description of the event, the containment strategy, required approvals, and the final status.

While an unauthorized removal of a message from the EX system has not yet occurred, if the audit reports were to indicate a message ID number other than the targeted data spill message had been deleted, the Records Management team would notify Information Security, the CIO, OA General Counsel, and the affected EOP component(s) Counsel's Office. Information Security would then begin an investigation and provide a course of action to restore the deleted data. A full report of the incident containing confirmation that the removed data has been restored to the EX repository is required which will then be distributed to the Records Management team, the CIO, OA General Counsel, and the affected EOP component(s) Counsel's Office.

The EX system is stored in an off-site, tight security, location where EOP employs the industry's best practices in the area of cyber security. EOP has employed the best industry cyber security advisors available. EOP's data center is in a highly controlled and monitored facility.

Finally, EMC configured and installed EX. EMC has confirmed that its installation complies with best practices. I have enclosed a letter from EMC Corporation's Chairman and CEO certifying that the system installed is accurately archiving EOP email. During the life cycle of the EX system EMC will provide configuration changes, security patches, and other support as required to maintain the integrity of the EOP's email archive.

The Office of the CIO will review and assess new technologies as they evolve to ensure we continue to provide the Executive Office of the President a secure and complete email archive system.

Sincerely,

Brook Colangelo
Chief Information Officer

W/ENCL