information
governance
initiative

iginitiative.com

May 1, 2015

The Hon. Charles Grassley
Chairman
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

The Honorable Patrick Leahy
Ranking Member
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Chairman Grassley and Ranking Member Leahy:

Thank you for the opportunity to provide a written submission for the record of the hearing "Ensuring an Informed Citizenry: Examining the Administration's Efforts to Improve Open Government."

I am writing as Co-Chair of the Information Governance Initiative, a vendor-neutral industry consortium and think tank established in 2014 dedicated to advancing the adoption of information governance practices and technologies through research, publishing, advocacy, education, and peer-to-peer networking.[1] The IGI considers it well within the scope of its mission to provide useful recommendations to public sector institutions on how state-of-the-art software in the information management space may be used in furtherance of important public policy goals, including compliance with the Federal Records Act and the Freedom of Information Act.

By way of further background, I had the privilege of spending 33 years in the federal service, including as a trial attorney and senior counsel in the Civil Division of the Department of Justice, and as Director of Litigation at the National Archives and Records Administration (NARA). Between 1992 and 1999, I acted as lead DOJ counsel in

[1] See www.iginitiative.com. The views expressed here are not intended to preclude the submission of additional or differing views by individual or organizational members of the IGI.

1271 avenue of the americas
suite 4300
new york, ny 10020

866 626 2917

info@igintiative.com

the litigation known as the "PROFS case," *Armstrong v. Executive Office of the President*,[2] a landmark case involving preservation of White House e-mail under the federal records laws. During my time at DOJ and NARA, I performed duties on numerous other high-profile lawsuits filed under the Freedom of Information Act (FOIA), Federal Records Act, and Presidential Records Act. I consider it the highest honor of my life to have had the opportunity to represent the United States as government counsel, defending on a nonpartisan basis policies advanced by the administrations of President Reagan through President Obama. The views I express here are those of a former government lawyer with extensive legal background and experience on federal recordkeeping and access issues, without regard to party or politics.

The present hearing is important for reasons that go far beyond the actions of one former Cabinet officer's compliance with federal recordkeeping and access laws. From the first day of his Administration, President Obama has highlighted the importance of openness and transparency in carrying out the activities of government.[3] More recently, in connection with his Memorandum on Managing Government Records, the President has underscored that "recordkeeping is the backbone of open government."[4] However, in light of the substantial publicity surrounding revelations that former Secretary of State Hillary Clinton used a private email network for the conduct of official government business,[5] I believe it would be helpful first to focus on what I would have imagined to be several well-established propositions under the FOIA and the Federal Records Act. After

---

[2] 1 F.3d 1274 (D.C. Cir. 1993). For a history of the case, see Jason R. Baron, "The PROFS Decade: NARA, E-mail, and the Courts," in Bruce Ambacher, ed., THIRTY YEARS OF ELECTRONIC RECORDS (Lanham, MD: Scarecrow Press 2003).

[3] See President's Memorandum Re Transparency and Open Government, dated January 21, 2009, https://www.whitehouse.gov/the_press_office/TransparencyandOpenGovernment/.

[4] President's Memorandum on Managing Government Records, 76 F.R. 75423 (Nov. 28, 2011), https://www.whitehouse.gov/the-press-office/2011/11/28/presidential-memorandum-managing-government-records.

[5] See, e.g., Michael Schmidt, "Hillary Clinton Used Personal Email Account at State Dept., Possibly Breaking Rules," *New York Times* (March 3, 2015), http://www.nytimes.com/2015/03/03/us/politics/hillary-clintons-use-of-private-email-at-state-department-raises-flags.html?_r=0.

1271 avenue of the americas
suite 4300
new york, ny 10020

866 626 2917
info@iginiative.com

doing so, I will make several observations and recommendations for the Committee's consideration regarding improving open government in the digital age.

First, the setting up of and maintaining a private email network as the sole means to conduct official business by email, coupled with the failure to timely return email records into government custody, amount to actions plainly inconsistent with the federal recordkeeping laws.

As an initial matter, any federal employee's decision to conduct *all* e-mail correspondence through a private e-mail network, using a non-.gov address, is inconsistent with long-established policies and practices under the Federal Records Act and NARA regulations governing all federal agencies. Ever since 1950, when Congress enacted the first comprehensive Federal Records Act, the head of each agency has been responsible for ensuring that adequate and complete documentation of the organization, functions, policies, decisions, procedures, and essential transactions of his or her agency is maintained.[6] This statutory obligation applies first and foremost to the records of the head of the agency him or herself. This obligation is routinely carried out through the implementation of official recordkeeping systems, adequate controls, and records schedules, all requiring that federal records be retained either permanently, or temporarily for set retention periods.[7] All high level officials are or should be aware of their basic obligations to maintain adequate documentation of their activities in government. No federal employee, including high-level officials, is allowed an "exemption" from these requirements.

In the wake of the 1993 federal court of appeals decision in the above-referenced *Armstrong* case, which held that the electronic versions of e-mails (including complete sender and recipient information) may be worthy of preservation as federal records, federal agencies have been governed by NARA's government-wide regulations covering e-mail record as first promulgated in 1995.[8] These regulations in their present form[9] require that all federal record e-mails appraised as long-term temporary or permanent

---

[6] See 44 U.S.C. 3101; see generally 44 U.S.C., Chapters 21, 29, 31 and 33.
[7] 44 U.S.C. 3303, 3303a.
[8] NARA Final Rule on Electronic Mail Systems, 60 F.R. 44641 (Aug. 28, 1995) (originally codified at former 36 C.F.R. 1234.24 (1995)).
[9] See 36 C.F.R. 1236.22 (2014) (text unchanged since 2009).

records, either be printed out or electronically transferred to an appropriate official recordkeeping system. (In 2006, the regulations were amended to make clear that short-term, transitory e-mail records may simply be left to reside on an e-mail network, prior to deletion.) Again, every federal employee including high-level officials has been governed by the obligation to preserve e-mail records documenting agency policies and decisions since 1995.

Specifically with respect to e-mail communications created or received outside of official electronic systems maintained by an agency, the 2009 NARA regulations state:

> Agencies that allow employees to send and receive official electronic mail messages using a system not operated by the agency must ensure that Federal records sent or received on such systems are preserved in the appropriate agency recordkeeping system.

Had I been asked to provide a legal opinion on the meaning of this regulation while in my former official capacity in NARA's Office of General Counsel, I can assure this Committee that I would have said that e-mail records sent or received on a private commercial network (e.g., on Gmail, or on one's own server), should be transferred contemporaneously with their creation or receipt, and certainly *no later than when an official or employee left public service.* This interpretation is especially reasonable in light of the fact that when exiting government service, federal employees are otherwise expected to have made an effort to ensure that federal records in their possession (including in work spaces in the case of paper records, or local hard drives or servers in the case of electronic records) are preserved in an appropriate official system. Every agency either has or should have employee "exit procedures" in place which take into account the need to preserve records. I believe the vast majority of federal records officers would interpret this regulation in the same manner as I do.

Last year, as part of Congressional enactment of the Presidential and Federal Records Act Amendments of 2014, section 2911 of the Federal Records Act was amended to expressly provide that an officer or employee may not create or send a record using a non-official electronic messaging account unless the e-mail is copied to or transferred to an official account within 20 days, with further provision for possible disciplinary

1271 avenue of the americas
suite 4300
new york, ny 10020

866 626 2917
info@iginiative.com

sanctions for intentional violations.[10] However, the fact that the 2014 statute sets an express deadline does not excuse tardy conduct under the 2009 regulations; if anything, the statute underscores the fact that the prior regulations were not intended or reasonably read to allow high-level officials to meet their obligations by returning records into government custody only when they chose to do so, perhaps many months or years after leaving office. The Federal Records Act has never given employees or officials that kind of license to evade their responsibilities in ensuring that adequate documentation of their time in the public service is preserved for the American people.

Indeed, the Federal Records Act contains provisions where an agency head or the Archivist of the United States is empowered to notify the Attorney General when federal records have been improperly removed from government custody or where a threat exists as to their destruction, for consideration of a possible "replevin" lawsuit to demand return of records that are rightfully the government's to possess and preserve.[11] Although this provision is discretionary, and would normally only be invoked where clear evidence exists that government records remain in the possession of a private citizen, it is a useful additional tool (beyond section 2911) in future cases where an official has departed from office with e-mail or other records in their possession, and a credible threat to their continued preservation exists.

Another aspect of the recent controversy has been the erroneous assumption on the part of some that e-mail records from a private or commercial account, when sent to or received from a ".gov" address, are being automatically preserved "somewhere" in a federal agency -- thus providing an excuse for the failure to have taken adequate steps to ensure that such records are transferred from a private account. There are several problems with this assumption. Very few federal agencies have implemented an automated system for archiving email. For example, at the State Department, the so-called "SMART" system apparently has been used in a fashion (at least until recently) where only a tiny percentage of e-mail communications were tagged as records in an electronic archive repository.[12] Moreover, to the extent federal agencies continue to rely

[10] See Pub. L. 113-187 (adding 44 U.S.C. 2911).
[11] See 44 U.S.C. 2905 & 3106.
[12] See State Department Office of Inspector General Report ISP-I-15-15, "Review of State Messaging and Archive Retrieval Toolset and Record Email," March 2015,

on "print to paper" policies for preserving email records, there is little assurance that over-burdened employees are able to comply with the manual efforts needed to ensure that those policies are routinely carried out.

Second, a federal employee or official choosing to carry out communications using a non-".gov" address, without making timely transfer of those records to an appropriate governmental system, compromises the ability of an agency to adequately respond to FOIA requests.

For example, the State Department, like every federal agency, struggles with attempting to keep up with the thousands of FOIA requests received and pending in its FOIA queues. To meet an agency's responsibilities to provide timely access to government records, in most instances FOIA officers must rely on custodians of records (i.e., actual end-users with individual e-mail accounts on an e-mail network) to locate responsive records to public access requests. Moreover, under the Electronic Freedom of Information Act Amendments of 1996, requesters have the right to demand that responsive records be provided in an electronic format.[13]

Whatever bureaucratic obstacles agencies have in responding to requests in a timely way, their duties are made hugely more difficult in the case of a high-level official choosing to exclusively maintain their e-mail record communications on a private network server. In this scenario, neither the FOIA officer nor the records officer has any direct means of access to records that may be responsive to individual requests. The FOIA officer may not even know of the existence of the private server, as he or she would not routinely be a close confidant or in the circle of advisors of such an official.

The erroneous assumptions made with respect to automated archiving apply as well to access considerations under the FOIA. The fact that an e-mail sent to or received from a ".gov" address existed at some point on a government e-mail network does not automatically ensure that the e-mail would have been printed out or otherwise archived for preservation in an official recordkeeping system, so as to be available for access through FOIA. Moreover, if e-mail records from a private server or commercial account

---

https://oig.state.gov/system/files/isp-i-15-15.pdf (stating that only approximately 60,000 out of 1 billion e-mails sent in 2011 were tagged as federal records).

[13] See 5 U.S.C. 552(a)(3)(B), as amended by Pub. L. 104-231.

were sent to or received from a .gov locations outside the agency in which the employee or official works, they would only be available to FOIA request lodged at that separate federal agency. But an e-mail from a Cabinet officer concerning official business would in the normal course be considered a federal record in both the sender agency as well as the recipient agency, and hence would be expected to be an "agency record" within the definition of the FOIA, and accessible to the public if a request were filed in either location.

Third, the recordkeeping laws narrowly circumscribe what is truly to be considered "personal records." Pursuant to NARA regulations, "If information about private matters and agency business appears in a received document, the document is a Federal record."[14]

In other words, when high level officials take it upon themselves to decide what is personal, and what are official records, to be transferred from a private or commercial account, NARA's default rule should be applied essentially in this manner: where *any paragraphs or sentences* in a given e-mail pertain to government business, the e-mail is to be considered a "federal record" to be transferred to an appropriate recordkeeping system for preservation, for future possible release under FOIA in whole or in part.[15]

Federal employees make decisions every day as to what e-mail records should or should not be preserved in accordance with agency recordkeeping policies, and it is not wrong for an employee to exclude personal e-mails sent or received on a government system from what are otherwise the rules for preserving federal records. However, in the usual course, agency employees are making these types of decisions with respect to communications sent or received on a government electronic system. This means that their choices in archiving e-mail are capable of oversight, by supervisors, records managers, Inspectors General, or others with authorization to conduct audits or inspections. In contrast, the routine use of commercial e-mail services for government business (including the setting up of a private network) potentially cloaks in secrecy all

---

[14] 36 C.F.R. 1222.20(b)(2).

[15] Any portions of email records deemed "personal" can be withheld at the agency's discretion under Exemption 6 of the FOIA, 5 U.S.C. 552(b)(6), on the grounds that release would constitute a substantial unwarranted invasion of privacy.

1271 avenue of the americas
suite 4300
new york, ny 10020

866 626 2917
info@iginiative.com

decision making with respect to what is personal and what is official, without further oversight.

Concededly, the 2014 Amendments (as well as the 2009 NARA regulations) leave to the federal official the responsibility to decide which e-mail communications created or received on a non-governmental account constitute federal records to be transferred to an official recordkeeping system. In small numbers, this can be accomplished routinely by an official on a contemporaneous basis, as Congress assumed when enacting the 20 day provision in current law. But in my view, neither the 2014 Amendments nor NARA's 2009 regulations reasonably contemplate leaving to an ex-official, in the absence of any oversight by a records officer or otherwise, the unilateral decision to delete large numbers of email records as personal -- absent some assurances in advance that the default rule stated above has been properly applied. Under such circumstances, interested parties are forced to simply trust that the employee or official has acted in good faith in a manner consistent with NARA's default rule, lest portions of the historical record are missed.

Further Observations and Recommendations

Over the past twenty-five years, as agencies have moved into the digital age, they have provided employees with the ability to communicate through numerous electronic communications networks, both as set up in-house, as well as through means of the Internet. Every major agency now maintains one or more e-mail systems on which a large number of official communications meeting the definition of what constitutes a 'federal record" are created and received. Some estimates are that tens of billions of e-mail communications are sent and received each year across the government; if even a small fraction of these constitute "permanent" records of the United States worthy of preservation in the National Archives, agencies must put into place adequate recordkeeping policies and controls to account for these records.

The present controversy involving a private email network appears to have been at least partially based on faulty assumptions about the state of government recordkeeping – that messages on a private network would nevertheless be archived by others in the normal course. Because that is not routinely the case, this Committee would do well to focus its attention on how electronic recordkeeping can be improved, in order both to

preserve our history, as well as to improve citizen access to governmental decision-making.

In response to President Obama's 2011 Memorandum, Archivist of the United States David S. Ferriero, and OMB's then-Acting Director Jeffrey D. Zients, issued a Managing Government Records Directive in 2012 that presents a path forward for federal agency compliance with recordkeeping obligations in the digital age.[16] In accordance with the Directive, by December 31, 2016, all federal agencies are to manage their e-mail records in accessible electronic formats.[17] If implemented, the Directive means the end of "print to paper" policies for official recordkeeping of e-mails.

In addition, the Directive calls for agencies to meet a December 31, 2019 deadline for ensuring that future permanent federal records created or received after that date will be managed electronically to the fullest extent possible for eventual transfer and accessioning into the National Archives. In other words, after 2019, the Archivist of the United States intends that the National Archives not accept paper records initially created after that date – only "legacy" paper records from earlier decades will continue to be accepted. This Directive represents an inflection point in the history of archives, and helps to ensure greater preservation of our Nation's history in a digital age.

Congress also has acted to underscore the importance of the Archivist's Directive in enacting the 2014 Amendments, which amend section 2904(d) of the Federal Records Act to provide for the Archivist to issue regulations requiring federal agencies to transfer all digital or electronic records to the National Archives in digital or electronic form to the greatest extent possible.[18]

To help implement the 2016 and 2019 mandates, NARA has published recent guidance on how "Capstone" policies for e-mail may assist agencies in meeting their record obligations.[19] In a nutshell, Capstone represents an approach to e-mail management

---

[16] See M-12-18 (August 24, 2012), https://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-18.pdf.
[17] *Id.*, section 1.2.
[18] See H.R. 1233, section 9, amending 44 U.S.C. 2904(d).
[19] See NARA Bulletin 2013-02, "Guidance on a New Approach to Managing E-Mail Records,"

that relies on the automated archiving of e-mail records with a minimum of end-user involvement. Senior officials in federal agencies, with designated "Capstone accounts," will have all of their e-mail records presumptively deemed to be permanent federal records. Everyone else at agencies adopting a Capstone framework would have their e-mail records captured in a repository for a designated "temporary" period of time – which might end up being many years. NARA has a draft General Records Schedule for agencies electing to be covered under Capstone that calls for all e-mail records to be preserved for a minimum of seven years (with senior officials' e-mail records preserved permanently).[20]

The Archivist's Directive and NARA's Capstone approach to e-mail management go a long way to solving existing defects in current agency e-recordkeeping practices. Recent controversies involving e-mail records at the IRS, as well as the present controversy, may not have happened in the same way if agencies previously had taken the initiative to ensure the automatic archiving of employees' (and especially senior officials') e-mail records in a shared official repository – instead of having to rely on reconstruction or restoration of failed hard drives, backup tapes, or recovery of records from private servers.

It remains to be seen whether senior officials across government treat as a priority meeting the 2016 and 2019 recordkeeping mandates. This Committee will perform a very useful function in monitoring the progress of agencies in meeting their recordkeeping obligations under the Directive. If agencies adopt Capstone policies for electronic archiving of e-mail, and other forms of electronic recordkeeping, they help to ensure that records in electronic form not only are preserved, but are also accessible to FOIA and other requestors.

To continue the momentum initiated by the Archivist's Directive and Congressional enactment of the 2014 Amendments, I respectfully submit the following three recommendations for the Committee's consideration.

---

dated August 29, 2013, http://www.archives.gov/records-mgmt/bulletins/2013/2013-02.html.

[20] See proposed GRS 6.1, "Email Managed Under A Capstone Approach," http://blogs.archives.gov/records-express/2015/04/02/draft-capstone-grs-available/.

1. Directing Inspectors General across government to pay greater attention to how their respective agencies are meeting the Archivist's 2016 and 2019 mandates, including providing Congress with updates in semi-annual reports. IGs ideally perform very useful functions in providing regular audits and oversight on how agency programs and policies are implemented, which if they chose to do so, could well include heightened reviews of agency progress in implementation of the Directive's mandates.

#2. Requiring OMB to ensure that as agency officials move to "cloud-based" platforms for storage of government data, they specifically take into account how their agencies will embed records management obligations and provide for FOIA access to data constituting federal records. Government-wide, it is far from self-evident that "cloud-first" policies in managing data also satisfactorily have accounted for federal recordkeeping requirements and FOIA considerations.

#3. Establishment of an Electronic Records Advisory Committee reporting to the Archivist of the United States and the Office of Management and Budget, tasked with the mission of issuing benchmark reports on what progress the government is making in meeting the 2016 and 2019 mandates, and issuing recommendations as appropriate. In particular, the Advisory Committee could be tasked with reporting on how agencies are thinking about integrating the ability to meet FOIA's requirements as part of their planning efforts to meet the 2016 and 2019 recordkeeping mandates.

The recent controversy with respect to maintenance of a private email network represents a "teaching" moment for the government, in which recordkeeping and open government issues are recognized for their importance. The history of the United States, and the availability of the government's records in electronic form for a better informed citizenry, could not be more important to recognize. We should be able to learn from recent events in urging senior federal officials to continue making progress towards ensuring a more open government in the digital age.

1271 avenue of the americas
suite 4300
new york, ny 10020

866 626 2917
info@iginiative.com

I wish to thank the Committee for the opportunity to provide these views.

Sincerely,

Jason R. Baron
Co-Chair
Information Governance Initiative
jason.baron@iginitiative.com
(202) 230-5196

Biographical Statement

I served as a trial lawyer and senior counsel in the Federal Programs Branch, Civil Division, DOJ, between 1988 and 1999, and was a trial lawyer at the Department of Health and Human Services prior to that. Beginning in 2000, I served as the first Director of Litigation in the Office of General Counsel of the National Archives and Records Administration. By way of further background, I have been honored with over 20 awards and commendations during my time in public service, including from the Archivist of the United States, the Justice Department, the National Security Council, and the Department of Health and Human Services. I am the recipient of the 2013 Justice Tom C. Clark Outstanding Government Lawyer Award given by the D.C. Chapter of the Federal Bar Association, as well as of the internationally recognized 2011 Emmett Leahy Award (the first federal lawyer honored in the 40 years the award has been given), for lifetime career achievements in records and information management. I have authored dozens of scholarly papers and commentaries on the subjects of electronic recordkeeping and e-discovery, and have given over 400 presentations around the United States and the world on issues involving the preservation of e-mail and other forms of electronic records. I have served as Co-chair of The Sedona Conference® Working Group on Electronic Document Retention and Production, am presently on the boards of the Georgetown Advanced E-Discovery Institute and the Cardozo Data Law Initiative, and am also presently Chair-elect of the D.C. Bar Litigation Section's E-Discovery Committee. I have also served on the Board of Directors of ARMA International. In October 2013, I joined the law firm of Drinker, Biddle & Reath LLP, in Washington, D.C., where I practice in the Information Governance and eDiscovery Group, and serve as Co-chair of the Information Governance Initiative. I am also an Adjunct Professor at the University of Maryland's School of Information Studies, where I have taught the first e-discovery course for PhD and Masters candidates in the United States. I am a member of the District of Columbia and Massachusetts bars, as well as the bar of the Supreme Court. My full CV is available at http://jasonrbaron.com.