

June 2, 2011

Delivered via e-mail c/o Carla Stone, Office of Management and Budget (OMB)

Scott Bernard, Federal Chief Enterprise Architect, OMB

William Cira, Acting Director of the Information Security and Oversight Office

John Fitzpatrick, Director Special Security Center, Office of the Director of National Intelligence

Michael Howell, Deputy Program Manager for the Information Sharing Environment

Vivek Kundra, Federal Chief Information Officer (CIO)

Tim Nusraty, Attorney, General Counsel's Office, OMB

Dear Sirs:

We are writing to respond to your request that we provide you with some guidelines and principles that we believe will help you develop a 21st century framework of policies for governance of intra-government information sharing. Our organizations work on a variety of issues related to transparency, good government, and preserving civil liberties in the national security context. Although not all our organizations address all of the issues discussed below, we come together in urging policies that will promote openness and accountability.

While the WikiLeaks disclosures have brought to light serious weaknesses in our information safeguarding policies and procedures that must be addressed, we cannot afford to neglect various complementary, and sometimes competing, government interests like promoting efficient information-sharing, serving the public interest, protecting constitutional rights and the role of whistleblowers in uncovering fraud, waste, or abuse, and creating and maintaining robust checks and balances. These interests must be held in balance with measures taken to secure information.

Thus, security measures to address WikiLeaks-type scenarios and other cyber-security risks must be narrowly focused to target the identified risk. Unnecessarily broad policies and procedures could easily swing the pendulum too far: creating new incentives to overclassify information, diverting agency resources from actions needed to actually improve information security, creating excessive secrecy that contributes to rather than prevents leaks, and violating the rights of federal employees and others. Also, in many cases there cannot be a one-size-fits-all approach. Some practices used within the intelligence community are not applicable or appropriate for other agencies, and may not be properly protective of First Amendment speech rights and civil liberties, privacy and due process rights for employees in any agency.

We provide three broad areas for consideration while promulgating a new framework for information security, and lastly some thoughts about the framework itself:

Reduce the scope of the classified universe. Rampant overclassification, a problem that has been identified by numerous Congressional committees, Commissions, advisory groups, and by the President himself, undermines the integrity of the very system we depend upon to ensure that our nation's

adversaries cannot use national security-related information to harm us. Crafting policies and procedures to ensure that only information that legitimately needs protection is labeled as classified would create a more credible, agile and flexible classification system.

President Obama's January 2009 Executive Order (EO) on Classified National Security Information, EO 13526 (section 1.9), includes a mechanism to help curb overclassification of national security information through the Fundamental Classification Guidance Review process. Unfortunately, the process has produced no known results to date. We urge you to appoint a team responsible for monitoring and reviewing agency actions, and for setting measurable targets for reducing the size of the classified world. The team should also be aware of and, when appropriate, engaged in the Public Interest Declassification Board's (PIDB) work on transforming the classification process. Several of our organizations have submitted classification reform proposals to the PIDB. These proposals and those offered by PIDB members should be given close consideration.

Be mindful of federal employees' rights, especially as you create policies and procedures to address insider threats. Federal agencies must be required to have reasonable suspicion to initiate any investigation and/or collection of information about employees' personal lives and/or First Amendment-protected activities. Federal employees who blow the whistle on waste, fraud or abuse must have safe channels for disclosing wrongdoing and meaningful protections against retaliation. The Administration should issue an Executive Order creating a strong, independent whistleblower protection system for intelligence community and national security workers, and sending a strong message that retaliation against whistleblowers will not be tolerated.

As classified information is not only made public by entities like WikiLeaks, we urge you to provide clarity for federal employees about the current classification status of information that high ranking officials have shared with sources outside the government. Further, we suggest you consider the possible harm to national security caused by preventing public employees from using information that is freely available to our enemies. Insisting that federal employees blind themselves to any information that remains technically classified, but is clearly in the public domain, puts them at an information disadvantage.

Protect the public's right to know under the Freedom of Information Act (FOIA). As with President Obama's EO on Controlled Unclassified Information (CUI), it should be clear that any policy intended to improve information sharing within the government has no relationship to the ability to release the information under FOIA. They are completely separate processes. We urge you to provide clear guidance to federal employees regarding the Administration's expectations for proactive and discretionary releases of government information to the public, and to reinforce the message that CUI markings have no effect on FOIA.

In a March 31 letter, many of us urged the administration to coordinate and submit for review all agency proposals for new exemptions to FOIA.¹ Agencies already are seeking exemptions for information that they formerly withheld under the broad interpretation of FOIA Exemption 2 overturned by the Supreme Court in *Milner v Department of the Navy*. We urge you to ensure that agencies do not seek overbroad and unnecessary exemptions from public release or improperly use existing exemptions in response to your policies.

In addition to our thoughts on these specific issues, we have some thoughts on the infrastructure and processes you are building to manage information policy. In addition to the technology, intelligence and national security participants, there also should be participation by representatives from other government agencies and bodies with specific expertise in the range of issues related to balancing critical information security with checks and balances that protect public access to government information, civil liberties, whistleblower activities, and privacy rights. For example, representatives from the Open Government Working Group, FOIA community/OIP/OGIS, OSC, and DOJ should be included in the new government-wide collaboration. Once its members have been appointed and confirmed and it is finally operational, the Privacy and Civil Liberties Oversight Board created by legislation in 2007 could play a vital role in reviewing such policies. In the meantime, we urge you to dedicate at least one individual on your team to reviewing proposals with the goal of protecting civil liberties, privacy rights, and the public's right to know. We also greatly appreciate your consultation with us and other stakeholders/members of the advocacy community to date, and hope that you will continue to keep us apprised of your efforts as you progress, so that we may raise any concerns or suggestions in a timely manner.

We note that effective oversight of information governance is critically important. Accordingly, new policies and procedures should include the establishment of independent reviews and audits. In terms of their substance, these policies and procedures should avoid creating too many punitive measures.

We also suggest you closely monitor ad hoc attempts by Congress to address information sharing and safeguarding issues. While Congress has an important oversight role, the Administration should identify and actively oppose any proposals that could violate protected constitutional rights and privacy interests of employees and access rights for the public.

Finally, the first step in achieving the proper balance between information security and the privacy/access interests discussed above must be to fulfill your commitment to clarify the intent and appropriate application of the January 3 memo directing agencies to inventory their practices for safeguarding information in the wake of WikiLeaks.² You have acknowledged that it was not your intent to direct agencies to apply new practices listed in the checklist, such as monitoring employees' pre- and post-employment activities or participation in on-line media data mining sites like WikiLeaks and

¹ <http://www.openthegovernment.org/sites/default/files/Milner-coordinatedProcessFinal.pdf>

² <http://www.openthegovernment.org/sites/default/files/otg/CommentsOMBLEaksMemo-Final.pdf>

requiring employees to report all contact with the media, or to suggest that these measures represent “best practices.” You agreed that clarification on this point might be needed. We hope that you will soon make that official clarification to all agencies in writing to ensure that you are not encouraging agencies to craft policies that unduly restrict free speech or otherwise distract agencies from actually improving information security.

We appreciate your asking for our thoughts on principles to guide you as you develop a governance framework for 21st century intra-government information sharing, and we hope this is the beginning of an ongoing collaboration.

Sincerely,

Steven Aftergood, Director, Government Secrecy Program
Federation of American Scientists

Sharon Bradford Franklin, Senior Counsel
The Constitution Project

Angela Canterbury, Director of Public Policy
Project On Government Oversight – POGO

Tom Devine, Legal Director
Government Accountability Project –GAP

Mike German, Senior Policy Counsel
American Civil Liberties Union

Elizabeth Goitein, Co-Director, Liberty and National Security Program
Brennan Center for Justice

Patrice McDermott, Director
OpenTheGovernment.org

Sean Moulton, Director, Federal Information Policy
OMB Watch

Anne Weismann, Chief Counsel
Citizens for Responsibility and Ethics in Washington - CREW