"Secure Transparency": Why Cybersecurity is Vital to the Long-Term Success of Open Government

By Dan Chenok

For over two years, the Obama administration has pursued a pair of initiatives that have each, in different ways, impacted the management of government programs: open government and cybersecurity. At first glance, these initiatives appear to cover divergent topics, with only technology as a common element. Upon closer review, the advantages that open government creates will only be sustained through appropriately secure and agile information flows within and outside government. Similarly, security in cyberspace can be enhanced by a degree of transparency across all users that is not always adopted among security professionals; the more that non-expert managers and leaders understand the impact of good (or poor) protection, the better they will be able to use cyber assets responsibly. Government managers can leverage "secure transparency" to build strong and lasting programs based on sound use of information resources.

The Drive to Openness

The Open Government Initiative, kicked off by a presidential memorandum on Jan. 21, 2009 (www.whitehouse.gov/the_press_office/Transparency_and_Open_Government/) and expanded by the OMB directive of Dec. 8, 2009 (www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-06.pdf), has fostered a major expansion of information transparency, encourages citizens and businesses to leverage that information through greater participation in government policies and programs, and promotes ongoing collaboration in the development and operation of those policies and programs. Agencies have made information available under the Open Government Initiative (www.whitehouse.gov/open) on a wide variety of websites, including the landmark website www.data.gov and a modernized Federal Register that allows much easier government access and navigation (www.federalregister.gov).

Federal agencies continue to increase and improve their online connections with constituents. The Freedom of Information Act (FOIA, www.justice.gov/oip/foia_updates/Vol_XVII_4/page2.htm) makes it an affirmative obligation to release government data upon request unless doing so would be contrary to one or more statutory exemptions; a recent National Security Archive study of access to government through FOIA found good progress, though it indicated that much work remains (www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB338/index.htm). In an age when more immediate information is available to individuals than ever before, the federal government must continue to create avenues to address demand for data.

The Need for Protection

At the same time, the federal government must protect a significant amount of information including sensitive health and financial data, personally identifiable information, or law enforcement, homeland security, diplomatic, or classified data. It must be released carefully, in collaboration with state and local governments. The Wikileaks incident and its aftermath illustrate the dangers of unrestricted openness. While the vast majority of government information should be freely available, an important subset must be protected to carry out important public missions. In addition, the information

Dan Chenok is a Senior Fellow in the IBM Center for The Business of Government. He is responsible for thought leadership in the area of government technology and government management improvements. He also leads consulting services for Public Sector Technology Strategy working with IBM government, healthcare, and education clients.

systems that hold both open and protected information must be secure from vulnerabilities and threats in cyberspace.

Failure to address the security imperative could erode trust and confidence in open government in two major ways:

- If too much protected information is released improperly, government and business partners will be less likely to provide vital data, agency officials will be less likely to share that information across organizational boundaries, and citizens will be less inclined to participate by reporting information.
- If too many public-facing information systems are disrupted through a cyber attack or their information is compromised through cyber "exfiltration"—when an unauthorized party breaks into the system and takes data, but leaves the system operational so that it can come back for more—the online foundations of open government will be called into question as pressures mount to increase security walls and limit citizen access.

It is of paramount importance that federal agency open government teams, and the contractors and business

The Drive to Openness

Agencies have made information available under the Open Government Initiative on a wide variety of websites, including the landmark website www.data.gov and a modernized Federal Register that allows much easier government access and navigation, www.federalregister.gov.

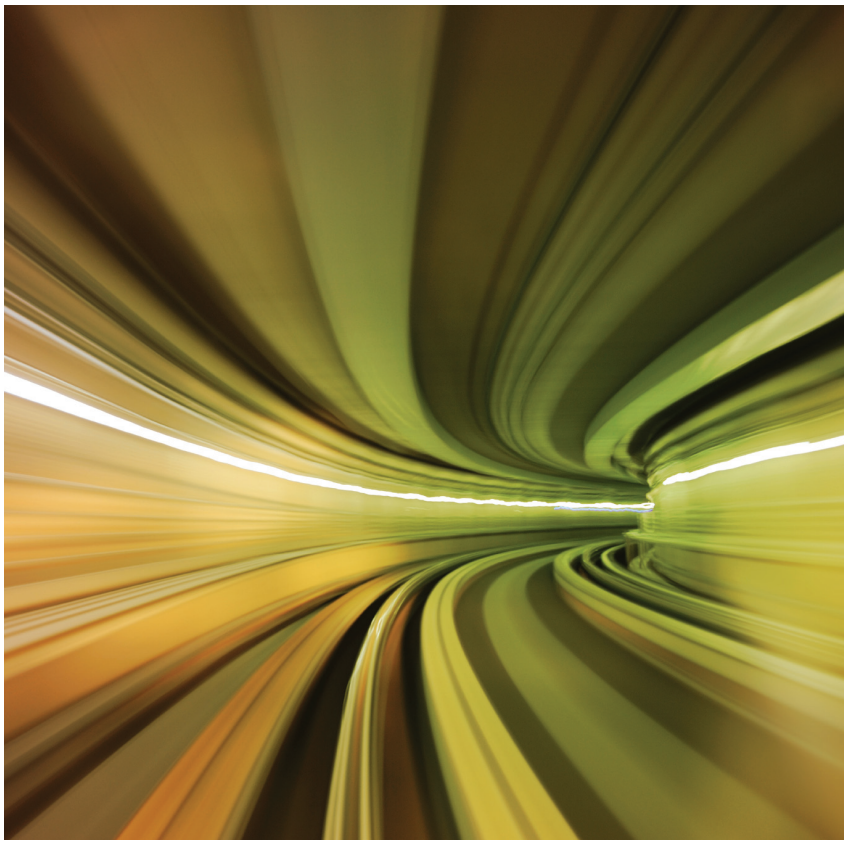
partners who support them, reach out to their colleagues in the security world to understand how they can build in data and system protections upfront. This will catch and correct most incidents before they become significant enough to cause a backlash that leads to restrictions on government information. Government managers today rely on the web and online databases to do much, if not most, of their jobs. Spending a little time on security in advance can save a lot of time spent responding to a major incident down the road, and can also allow the vast majority of open information to remain so over time.

Why Openness Helps Security

Generations of assurance professionals have been trained to only release information on a need-to-know basis. Since 9/11, agencies handling homeland security and terrorism data have made great strides in sharing secure information across previously impenetrable walls through programs like the Information Sharing Environment, operated out of the Office of the Director of National Intelligence, that promotes responsible sharing of terrorism information (www.ise.gov), and the recent exchange of personnel between the U.S. Department of Homeland Security and the U.S. Department of Defense to improve cybersecurity information sharing under a well-publicized memorandum of understanding (www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf).

These processes and initiatives illustrate an increasing collaboration across government and with the private sector. Part of an open government is collaboration, and key partners with federal agencies will be more likely to collaborate if there are secure channels for doing so. A good amount of attention is being paid by Congress to making these channels more workable and operational through statutory changes. Security officers should follow these developments actively to see how they can leverage previously unavailable resources to identify and respond to vulnerabilities and threats.

In addition, when everything is online, it is difficult to divide the workforce into "security" or "openness" or "program" camps. While there will certainly remain experts in each area, all three workforces have key skill sets for public leaders and managers—no one can succeed without the other. This makes it important for security teams to discuss the challenges and opportunities they can identify for collective responses, including training and awareness. Clearly, such conversations should be appropriate to the setting—specific threats and vulnerabilities would not be the first item on the agenda for a public training session—but security cannot succeed in the long run without more knowledge at all levels—workforce, citizen, business partner, and intergovernmental communities.



The Obama administration's National Initiative for Cybersecurity Education—carrying the easily memorized acronym of "NICE" (http://csrc.nist.gov/nice)—is focused on increasing cybersecurity awareness and education. More visible intersection between NICE and the Open Government Initiative would benefit both.

Secure Transparency Going Forward

A key mission of government is the collection, assessment, and dissemination of information. The increasing presence of cyberspace in daily life multiplies the quantity and visibility of public data. Protecting the systems that hold federal information, ensuring that mission-critical data are shared in a secure manner, and making citizens aware of what they can do to enhance the integrity of government in a cyber world are all key to effectively moving government programs forward toward secure transparency. Together, these measures can make secure transparency part of the means by which government achieves its objectives as more and more activity moves online. ◘