GOVERNMENT PERFORMANCE

CHAPTER 14

AMERICANS CAN CHECK THEIR BANK ACCOUNTS, COMMUNICATE WITH CUSTOMER SERVICE representatives and do their shopping anytime, anywhere by using applications enabled by broadband. Americans now expect this level of service from their government and are often disappointed with what they find. While some bright spots exist around filing taxes and paying parking tickets, these are the exception, not the rule. Government has fallen behind the private sector in using broadband to deliver services, and it is time to catch up.[1]

From city hall to the U.S. Capitol, government can better serve the American people by relying more on broadband. The implications are enormous.

The federal government can use broadband to increase the efficiency of its own internal operations. And it can use its size and purchasing power to help state and local governments and communities deploy more broadband capability.

Consider also the impact on low-income families. At the moment, many Americans do not receive all the benefits for which they are eligible. The reasons are many, including the complexity of determining eligibility, as well as lengthy and repetitive applications. Integrating and streamlining processes can help low-income Americans receive all the safety-net benefits for which they qualify, and that has had a demonstrable effect on bettering their chances of getting out of poverty.[2] Meanwhile, government services will operate more efficiently with the paperwork reduction that broadband technology allows. And when caseworkers assigned to these families spend fewer hours filling out paperwork, they can become more personally involved in helping their clients.

Broadband, in short, can change the way government serves the public. This chapter makes recommendations to accelerate this change. Section 14.1 focuses on how the government can take action to improve deployment of broadband in local communities. Section 14.2 proposes ways that broadband can improve government performance and service delivery. It also makes recommendations related to strengthening cybersecurity.

RECOMMENDATIONS

Improve connectivity through government action

- Federal government agencies and departments should serve as broadband anchor tenants for unserved and underserved communities.
- When feasible, Congress should consider allowing state and local governments to get lower service prices by participating in federal contracts for communications services.
- The Office of Management and Budget (OMB) should review and coordinate federal grants that have a broadband connectivity requirement. Federal government grant funding should not limit or permit limitations on the use of federally funded facilities or services for broadband deployment, except when technology solutions cannot ensure privacy or security of data.
- The Executive Branch and Congress should consider using federal funding to encourage cities and counties to gather information on initiatives enabled by broadband in ways that allow for rigorous evaluation and lead to an understanding of best practices.

Enhance internal government efficiency

- OMB should develop a vision and strategy to guide agencies on cloud computing.
- OMB and the Federal Chief Information Officers (CIO) Council should develop a competition to annually recognize internal efforts to transform government using broadband-enabled technologies.
- The Executive Branch should create an interagency working group, comprised of the senior grants officials from each agency, to implement guidelines and requirements for interagency coordination of grants and to improve Grants.gov to make it easier for applicants to use.
- The Federal CIO Council should accelerate agency adoption of social media technologies for internal use.

Strengthen cybersecurity

- The Executive Branch, in collaboration with relevant regulatory authorities, should develop machine-readable repositories of actionable real-time information concerning cybersecurity threats in a process led by the White House Cybersecurity Coordinator.
- The federal government should take an active role in developing public-private cybersecurity partnerships.
- The Executive Branch should expand existing and develop additional educational programs, scholarship funding, training programs and career paths to build workforce capability in cybersecurity.
- The Executive Branch should develop a coordinated foreign cybersecurity assistance program to assist foreign countries

in the development of legal and technical expertise to address cybersecurity.

- The FCC should work with Internet service providers (ISPs) to build robust cybersecurity protection and defenses into networks offered to businesses and individuals without access to cybersecurity resources. ISPs that participate in this program should receive technical assistance from the federal government in securing their networks.
- OMB should accelerate technical actions to secure federal government networks.

Improve service delivery

- OMB and the Federal CIO Council should develop a single, secure enterprise-wide authentication protocol that enables online service delivery.
- The Executive Branch should establish MyPersonalData.gov as a mechanism that allows citizens to request their personal data held by government agencies.
- Congress should consider re-examining the Privacy Act to facilitate the delivery of online government services and to account for changes in technology.
- The federal government should undertake a series of efforts to improve the delivery of government services online.
- The Executive Branch's review of the Paperwork Reduction Act should aim to enable government to solicit input to improve government services.
- The White House Office of Science and Technology Policy (OSTP) should develop a five-year strategic plan for online service delivery.
- The federal government should improve the delivery of means-tested benefits to low-income Americans.

14.1 IMPROVING CONNECTIVITY THROUGH GOVERNMENT ACTION

The federal government spends billions of dollars annually on broadband connections for its office buildings and facilities throughout the United States and provides billions more in funding for programs that have a broadband communications component. The government does not, however, leverage that spending in a coordinated way to improve broadband connectivity and access within local communities. In many cases, doing so would have a nominal incremental cost, but the impact on communities, especially those that are unserved or underserved, could be transformative.

Government can help in the deployment of broadband by serving as an anchor tenant in unserved and underserved communities, by leveraging the purchasing power of the federal government to provide lower prices for broadband communications services for state and local governments and by coordinating federal grants with a broadband connectivity requirement.

RECOMMENDATION 14.1: Federal government agencies and departments should serve as broadband anchor tenants for unserved and underserved communities.

State and local governments have expressed a strong desire to share broadband communications infrastructure deployed by the federal government to extend broadband connectivity to state and local agencies as well as unserved and underserved communities.[3] In response to Section 414 of the Transportation, Treasury, Independent Agencies, and General Government Appropriations Act of 2005,[4] the President directed federal departments and agencies to deploy redundant communications links for all facilities.[5] Implementation efforts did not account for the potential spillover benefits to people and businesses in unserved or underserved communities that are allowed to tap into the high-speed connection to the Internet that the government secured for its facilities. In the future, when deploying redundant links, the federal government should consult with local communities and use those links to extend broadband access to the unserved and underserved.

RECOMMENDATION 14.2: When feasible, Congress should consider allowing state and local governments to get lower service prices by participating in federal contracts for communications services.

The federal government is one of the largest buyers of products and services in the country, especially when it comes to information technology (IT). Since passage of the E-Government Act of 2002,[6] state and local government entities have been authorized to leverage the bulk purchasing power of the federal government to purchase a wide variety of information technology hardware, software and services. Use of that authority has increased every year, and state and local governments have saved millions of dollars. Purchasing authority is, however, restricted to items found on the General Services Administration (GSA)'s IT Schedule 70.

In 2007, GSA negotiated a 10-year, $68 billion telecommunications and network services contract to provide voice, IP, wireless, satellite and IP-centric services to 135 federal agencies operating out of 191 countries, at rates that are 10-40% lower than in previous contracts. This contract, called Networx, includes a provision that allows state and local governments to utilize the contract if federal law is changed to allow the practice.

Congress should consider allowing state and local governments to take advantage of Networx and other communications contracts to enable cost savings and encourage broadband deployment.

RECOMMENDATION 14.3: The Office of Management and Budget (OMB) should review and coordinate federal grants that have a broadband connectivity requirement. Federal government grant funding should not limit or permit limitations on the use of federally funded facilities or services for broadband deployment, except when technology solutions cannot ensure privacy or security of data.

In certain cases, well-intentioned grant programs require that money be spent on broadband connections even though a review of other projects would show that spending to be redundant.[7] Sometimes, a broadband connection already exists. In other cases, multiple grants may be used to build multiple connections. For example, grants for primary and secondary education networks and grants for rural health care networks often call for the development of independent networks, even though one would suffice.[8] Coordination at the OMB level would greatly reduce inefficiencies in federally-financed broadband rollouts.

RECOMMENDATION 14.4: The Executive Branch and Congress should consider using federal funding to encourage cities and counties to gather information on initiatives enabled by broadband in ways that allow for rigorous evaluation and lead to an understanding of best practices.

Examples abound of potentially powerful initiatives including IBM's Smart Cities,[9] Cisco's Connected Communities[10] and Google's proposed 1 Gbps fiber-to-the-home "broadband testbed."[11] These initiatives use broadband connections to try to solve some of today's most challenging public policy problems in areas such as transportation, health care, education, public safety and government services. Dubuque, Iowa, is reducing water and electricity use by deploying sensors connected via broadband. Alameda County, California, has implemented an integrated data warehouse for social services that saves $11 million a year by reducing duplicative work and improving detection of fraud. Unfortunately, information on projects like these is not collected systematically.

Federal broadband grant programs can fill the gap by including reporting requirements for recipients.[12] Gathering the information will not only help the federal government set priorities when issuing grants but also will assist local governments in identifying best practices across the nation.

Executive Branch agencies should run these initiatives like pilot programs and evaluate their success against pre-established benchmarks. This would help inform the next set of Congressional actions to promote widespread adoption of the techniques that prove successful with the pilots.

14.2 IMPROVING GOVERNMENT PERFORMANCE

Innovative applications of broadband have transformed the private sector, creating countless new ways of collaborating with partners and interacting with customers. Government, however, has not kept pace.

A poll of U.S. citizens by the Pew Research Center for the People & the Press found that in 2007, 62% agreed that government is usually inefficient and wasteful, up from 53% in 2002.[13] This gap may be widening in part because the private sector has raised expectations that government has not met. While customers increasingly can go online to interact with private companies, the public still mostly deal with government via mail or in person, standing in line. While companies have made it easy for customers to find what they want, the government has been slow to adopt technological efficiencies to speed citizen service and eliminate its siloed structure.[14]

Smarter use of broadband can facilitate a vast change in government. Like private companies, government can make its services available 24 hours a day, seven days a week, 365 days a year. Broadband-enabled online services can create paths across government's bureaucratic silos so that someone wanting to access unemployment benefits can deal with the local government and the federal government at the same time. Broadband holds the potential to move all government forms online, eliminating paperwork. Broadband allows for online tutorials for simple government services, which can help free government employees to focus on the most complicated cases. And broadband can increase efficiency by increasing the speed and depth of cooperation across departments and across different levels of government.

Enhance Internal Government Efficiency

In government, historically siloed institutions have bred siloed systems that are inefficient. Through strategic use of broadband-enabled technologies, the federal government has the opportunity to become a model of efficiency and performance.

RECOMMENDATION 14.5: OMB should develop a vision and strategy to guide agencies on cloud computing.[15]

During the past decade, federal spending on information technology has grown substantially. On IT infrastructure alone, the federal government spends $20 billion per year.[16] The number of federal government data centers has more than doubled over the last 10 years from 493 to more than 1,200.[17]

Cloud computing has the potential to at least slow the growth in federal spending while increasing efficiency. A study by Booz Allen Hamilton estimates that an agency that migrates its infrastructure to a public or private cloud can achieve savings of 50-67%.[18] For example, the District of Columbia recently moved toward using a commercial cloud computing solution for its mail, calendar, instant messaging, word processing and spreadsheet needs. The cost was only $50 per user per year; the District's previous solution for enterprise e-mail alone cost $96 per user per year.[19]

The federal government has already launched a number of limited cloud computing initiatives, with positive results. Electronic payroll systems have been consolidated from 26 systems to four shared-service provider centers; this will result in estimated savings of more than $1 billion during the next 10 years.[20] Apps.gov has allowed agencies to nimbly procure software and information technology services from GSA's Schedule 70[21] and deploy these solutions in the cloud. Agencies such as the U.S. Department of Defense (DoD) and the Central Intelligence Agency are also moving forward on internal cloud solutions for sensitive data.[22] The Rapid Access Computing Environment functions as an internal cloud for DoD, allowing for certification of applications that meet proper security standards within 40 days, half the time of the non-cloud-based method.[23]

Despite these successes, federal government IT executives harbor concerns about security and privacy. These concerns have some merit, but the risks can be mitigated through technology and policy solutions.[24] Because the risks many federal agencies face are the same, they would benefit from a community approach. OMB should develop a coordinated vision and strategy that touches upon the security and privacy policy concerns that must be resolved as the government moves to deploy cloud computing.

RECOMMENDATION 14.6: OMB and the Federal Chief Information Officers (CIO) Council[25] should develop a competition to annually recognize internal efforts to transform government using broadband-enabled technologies.

Federal government employees often generate ideas for innovation and efficiency within government, yet many of their ideas go unnoticed or unheralded. The federal government has taken initial steps to celebrate innovation and efficiency by launching the Securing Americans Value and Efficiency Award, a month-long contest that allowed every federal employee to submit ideas for how government can save money and perform better. The program received more than 38,000 suggestions.[26] The winning innovation was an idea to eliminate the waste of medications in VA hospitals.[27] This innovation has been included in the President's FY2011 budget, and agencies have been directed to implement many other recommendations resulting from the contest.[28] Expanding upon this, OMB and the Federal CIO Council should create a competition focused on transforming government operations using broadband-enabled applications.

RECOMMENDATION 14.7: The Executive Branch should create an interagency working group, comprised of the senior grants officials from each agency, to implement guidelines and requirements for interagency coordination of grants and to improve Grants.gov to make it easier for applicants to use.

During FY2009, the federal government awarded more than $1 trillion in grants.[29] Using broadband-enabled online services in the grant process can improve how the federal government implements its policies and programs.

Grants.gov was set up as a central portal for grants across the federal government to make the grants application process easier, but it has not succeeded on many metrics.[30] On average, federal government websites earn a satisfaction score of 75/100, but Grants.gov scores only 56/100.[31] Potential applicants must download forms to complete applications offline. There is no system for generating feedback about Grants.gov, limiting the ability to improve it.[32]

The proposed interagency working group should be empowered to recommend improvements to Grants.gov. Also, Grants.gov should allow tagging, or the labeling of grants, to make searches (especially of broadband grants) easier. This would enable the public to use USASpending.gov to gain a crosscutting view of all federal broadband expenditures while reducing the burden on applicants searching for grants.

The grant process should also be improved to require grantors to certify that any project requiring broadband has sufficient connectivity or that the funds from the grant would pay for that connectivity. Oversight for this process should rest with the interagency group.

RECOMMENDATION 14.8: The Federal CIO Council should accelerate agency adoption of social media[33] technologies for internal use.

Social media technologies provide the federal government another platform to spur innovation and collaboration. For example, the National Academy of Public Administration uses a wiki to synthesize interview data. This simple collaborative tool has reduced data analysis time by nearly 15%.[34]

The private sector has come to recognize the efficiency gains and other benefits of social media within the workplace.[35]

The federal government has not made widespread use of these tools despite evidence that federal government employees embrace the use of social media to make their organizations more efficient and effective. The Transportation Security Administration (TSA) uses a social media platform called IdeaFactory that allows its 43,000 officers to securely share ideas for improving their workplace and performance. TSA employees have submitted more than 9,000 ideas, generating more than 39,000 comments.[36] More than 40 ideas from IdeaFactory have been implemented, including changes to standard operating procedures.[37] The DoD has also embraced social media platforms to enhance internal efficiency, with 87% of DoD workers using these tools at work.[38]

Many agencies continue to have concerns about social media and block employee access to outside websites such as YouTube, Facebook and Wikipedia.[39] The Federal CIO Council has expressed concerns that these social technologies and tools could be susceptible to cyber attacks.[40] Still, there are clear benefits to adopting social media platforms for internal or cross-agency collaboration, and the Federal CIO Council should address concerns and accelerate adoption of these platforms (see Box 14-1).

Strengthen Cybersecurity

According to the Preamble to the United States Constitution, the federal government must "provide for the common defence" (*sic*). The United States has evolved dramatically since its founding, and one of the most significant changes that has marked the 21st century is the country's reliance upon the Internet in all sectors of society—from individuals to government to the economy at large.

The global, borderless nature of the Internet has also led to the emergence of new categories of threats that can come from anyone, anywhere in the world, at any time. Protecting the Internet and providing for cybersecurity is both an economic and national security challenge and collectively, one of the most serious challenges of the 21st century.[43] How the federal government approaches and provides cybersecurity will be critical to the continuing evolution of the Internet in the United States.

BOX 14-1:

The Intelligence Wiki

In 2006, members of the Intelligence Community formally launched the social media site Intellipedia to help solve information-sharing problems.[41] The effort has been well-received and is used by the Intelligence Community to share information classified up to "Top Secret." It now has more than 900,000 pages and 100,000 users who make 5,000 page edits every day.[42] Using Intellipedia, officials can quickly learn about new topics, scrutinize information and ensure it is up-to-date and complete.

The recommendations that follow apply to the federal government's approach to cybersecurity. Specific recommendations relating to the FCC and cybersecurity can be found in Chapter 16.

RECOMMENDATION 14.9: The Executive Branch, in collaboration with relevant regulatory authorities, should develop machine-readable repositories of actionable real-time information concerning cybersecurity threats in a process led by the White House Cybersecurity Coordinator.

The federal government recognizes that no operational mechanism currently exists for the United States to provide a "coordinated and unified effort to detect, prevent, mitigate, and carry out a real-time response to significant cyber issues affecting the Nation."[44] Recent real[45] and simulated events[46] demonstrate that responding to a cyberattack in real time is complex. Every second counts. Cyber threat detection, prevention, mitigation and response require coordinated action by public and private entities. In addition, traditional approaches to cybersecurity, including intrusion-detection systems and antivirus software, are ineffective against new rapidly evolving threats.[47] As a result, new methods are required to facilitate a coordinated response.

To begin addressing this challenge, the Executive Branch should develop machine-readable repositories containing actionable real-time information concerning cybersecurity threats (including signatures for viruses, spam, IP address blacklists and other indicators). By delivering information faster and in a more useful fashion, the Executive Branch will become an active partner in the public-private battle to protect cyberspace. These repositories will further facilitate timely interaction with both the private sector and international partners.

RECOMMENDATION 14.10: The federal government should take an active role in developing public-private cybersecurity partnerships.

- ➤ **The Executive Branch should develop protocols and incentives for establishing public-private cybersecurity partnerships with all major industry sectors. These protocols would enable sharing of cybersecurity information, threats, and incidents in a non-attributable manner, and would provide an existing channel for government to communicate actionable cybersecurity information to the private sector.**
- ➤ **The Executive Branch and the Small Business Administration should work together to develop a cybersecurity re-**

source program, in conjunction with state and local governments, to develop cybersecurity partnerships for small and medium enterprises (SMEs) that are not covered by cybersecurity partnerships developed for major industry sectors.

Cybersecurity continues to be a concern for the private sector in the United States, which relies on robust intellectual property protection to undergird its competitiveness. As a result, private sector networks in the United States, where most of its intellectual property resides, have been a major target for attacks, and despite the significant resources that the private sector devotes to cybersecurity, there have been a number of successful attacks on its networks. Recent victims of well-publicized cyber attacks include Google[48] and the U.S. oil industry.[49]

Due to the diffuse nature of cyberattacks, sharing of information is critical when responding to, mounting sufficient defenses against and remediating attacks. However, businesses are often reluctant to share information, either with other private sector entities or the government, due to worries about the potential disclosure of such an attack and related concerns about corporate liability, despite the fact that the resources necessary to successfully respond often exceed those of individual private sector organizations.

The public and private sectors must work together to overcome these challenges to ensure the security of the Internet. Information Sharing and Analysis Centers (ISACs), which convene a representative industry body to interact with the federal government on cybersecurity issues full-time, are good models for the kind of collaboration that is needed. Today, ISACs exist for the financial services sector (FS-ISAC), the information technology sector (IT-ISAC), and state and local governments (the Multi-State ISAC, or MS-ISAC). To ensure that ISACs for other industry sectors are effective, ongoing communication and actionable information will be required from both industry participants and the federal government.

SMEs often have fewer resources to dedicate to cybersecurity than large businesses in major industrial sectors. However, despite limited resources, cybersecurity is no less important to small and medium businesses. Recognizing both resource constraints and the importance of cybersecurity, the Executive Branch and the Small Business Administration should develop a cybersecurity resource program, in conjunction with state and local governments, through the MS-ISAC.

The effectiveness of public-private partnerships depends on ongoing communication and actionable information from both industry sector participants and the federal government. To ensure that this occurs, protocols and incentives should be developed for the sharing of cybersecurity information, threats and incidents in a non-attributable manner.

RECOMMENDATION 14.11: The Executive Branch should expand existing and develop additional educational programs, scholarship funding, training programs, and career paths to build workforce capability in cybersecurity.

Cybersecurity is a rapidly evolving field, requiring specialized training and expertise. The importance of this field to the economy, competitiveness and national security underscores the need to build a robust and capable workforce with the skills to sustain it. The federal government has an additional challenge in retaining skilled IT security officials because training and career advancement opportunities are limited.[50] However, the quality of professionals in the field of cybersecurity is mixed, with current training insufficient to meet the needs of either the public or private sectors.[51]

Immediately following the launch of Sputnik, governments in both the United States and Western Europe were deeply concerned about the growing quantity and quality of scientists and engineers in the Soviet Union. One of the major policy actions to address this concern was education and training in basic science, laying the groundwork for the United States' Apollo mission to go to the moon. Similarly, to meet the security challenges of the present day, a new professional cybersecurity workforce needs to be cultivated. The Executive Branch should expand existing and develop additional educational programs, scholarship funding, training programs and career paths to build workforce capability in cybersecurity. The Executive Branch should increase its current funding for these efforts.

RECOMMENDATION 14.12: The Executive Branch should develop a coordinated foreign cybersecurity assistance program to assist foreign countries in the development of legal and technical expertise to address cybersecurity.

The Internet knows no geographic boundaries, and threats and attacks emanating from cyberspace can come from anywhere at any time. The volume of cyberattacks originating internationally continues to grow.[52] To respond to these attacks effectively, a global response involving both the U.S. and foreign governments is necessary.[53] Although the U.S. government has been working to address cyber incidents through legal and policy actions and public-private partnerships many foreign countries lack either the legal framework or the capacity to respond in a similar manner.

To address this challenge, as it has done in cases of counternarcotics and human trafficking, the federal government must work collaboratively with international partners to address detection, prevention, mitigation and response with respect to cybersecurity. The International Criminal Investigative Training Assistance Program at the Department of Justice is an example of one program that works with foreign governments to develop professional and transparent legal institutions, with a focus on protecting human rights, combating corruption and reducing the threat of transnational crime and terrorism.[54]

Each federal government agency[55] with expertise should work collaboratively with its counterpart agencies in foreign governments to nourish the worldwide development of legal and technical cybersecurity expertise. In 1999, the U.S. led a similar collaborative effort to develop global expertise in telecom regulation, leading to the publication of *Connecting the Globe: A Regulator's Guide to Building a Global Information Community*.[56] A similar effort should be undertaken by the United States government in cybersecurity, bringing multiple countries together to share information on best practices.

RECOMMENDATION 14.13: The FCC should work with Internet service providers (ISPs) to build robust cybersecurity protection and defenses into networks offered to businesses and individuals without access to cybersecurity resources. ISPs that participate in this program should receive technical assistance from the federal government in securing their networks.

Protecting computers and other devices from new and evolving threats found on the Internet is a full-time activity that occurs 24 hours a day, seven days a week. Most Fortune 500 companies spend millions of dollars annually on specialized staff and technology supporting cybersecurity efforts to protect their corporate computers and networks. Smaller businesses and individuals, however, may have limited or even no cybersecurity protection.

ISPs have taken some steps to provide cybersecurity resources to small business and residential customers. For example, Comcast has provided a commercial antivirus and security software suite for free to customers since 2005[57] and will alert customers if their computers are infected with botnets, viruses or other online threats.[58] But these efforts only offer incomplete protection at best, since antivirus and security software may miss up to 80% of previously unknown Internet threats and attacks.[59]

As cybersecurity becomes increasingly specialized and technologically complex, it is no longer reasonable to expect that small business and individuals can engage in self-help when it comes to cybersecurity. By having ISPs take a more proactive role in securing their networks, Internet security can be enhanced, especially since the top 23 ISPs in the United States represent over 75% of all U.S. Internet subscribers.[60] Building upon efforts already taken by ISPs, the FCC should work with ISPs to build robust cybersecurity protection and defenses into networks offered to business and individuals. Participation by end-users would be voluntary: ISPs could offer a choice to subscribers between a network with built-in cybersecurity protection or a network with no cybersecurity protection. The FCC should identify ways that the federal government can provide ongoing technical assistance to secure these networks as an incentive for participation in this program.

RECOMMENDATION 14.14: OMB should accelerate technical actions to secure federal government networks.

Under the Federal Information Security Management Act (FISMA), OMB, through the Federal Chief Information Officer (CIO), has responsibility for securing all federal networks, except those under the purview of DoD and the Intelligence Community. OMB has undertaken a number of technical efforts to secure its networks. The Federal Desktop Core Configuration, a common platform for end-user computers, has been rolled out throughout the federal government and incorporates a standard information security configuration developed by the National Institute of Standards and Technology (NIST) in collaboration with DoD and the Department of Homeland Security (DHS).[61] The Trusted Internet Connections initiative is reducing the number of federal government Internet connections from over 8,000 connections down to approximately 50, and then deploying security solutions—including antivirus, firewall, intrusion detection, and traffic monitoring—on the remaining connections.[62]

In addition to these initiatives, further steps can be taken to bolster the federal government's cybersecurity efforts. The Federal CIO should accelerate technical steps to secure these networks and better position the federal government to react swiftly to new attack vectors. Particularly, the Federal CIO should speed the implementation of Internet Protocol Version 6 throughout federal government computer networks as a step towards implementing Internet Protocol Security and computer security at the network level. The Federal CIO should also accelerate efforts to securing the Internet's routing system.

OMB recently automated the FISMA data collection process, reducing the burden on agencies for FISMA compliance. Automating the data collection process will also allow the Federal CIO to more readily ensure FISMA compliance and improve existing benchmarks towards outcomes-based metrics so that federal agencies are taking all steps necessary to secure federal government IT networks.[63] Moving towards outcomes-based metrics is vital to securing the nation's critical infrastructure.

Improve Service Delivery

Americans can have a high-performance government that delivers many services online. But to realize this vision, technical and structural barriers must be addressed, including finding secure ways to establish identity and share information across agencies. Many government services rightly require identity authentication, such as presentation of a driver's license when applying for a U.S. passport. Additionally, government agencies must be able to share information across departments, with appropriate privacy safeguards, in order to reduce the burden on the public requesting government services.

In addition to removing these barriers, the government can improve service delivery by leveraging broadband-based tools to support the improvement, integration and modernization of federal government processes.[64] Low-income Americans accessing government benefits and services must navigate a fragmented world. They deal with multiple agencies and a host of forms. They typically must make in-person visits. A U.S. Government Accountability Office (GAO) report found that a family seeking to apply for the 11 largest means-tested benefits programs—including Temporary Assistance for Needy Families (TANF), food stamps, Medicaid and school meals—would have to complete six to eight applications and visit as many as six government offices. The process often requires many unpaid hours away from work and lengthy commutes.[65] A government employee on the other side of the desk spends hours per day entering data into antiquated systems that do not allow the kind of data sharing that could save money, improve productivity, reduce error rates and improve outcomes.

RECOMMENDATION 14.15: OMB and the Federal CIO Council should develop a single, secure enterprise-wide authentication protocol that enables online service delivery.

A robust, secure authentication protocol would enable new online government services as well as improvements to existing online government services, like online passport applications and electronic receipt of benefits. Such a system would enable a single sign-on so that individuals could access their college loan and tax information without creating multiple digital identities.

The federal government has released a strategy for development of secure authentication services for federal employees called the Federal Identity, Credential, and Access Management (ICAM) Roadmap.[66] In addition, the federal government has moved forward with limited implementation of an OpenID[67] pilot to provide public services requiring the lowest assurance level, or "little or no confidence in the asserted identity's validity."[68] Consider that a webmail account has some security and is associated with some identity, but because it is simple to claim any name one wishes, there is "little or no confidence" that an email from "John Doe" is indeed from a person named John Doe. OpenID enables simple applications such as using existing credentials (for example, with a webmail account) to provide individual customized Web-page functionality[69] for the National Institutes of Health (NIH) and other agencies. NIH is also currently testing applications with higher levels of identity assurance that draw on information from providers like Equifax and PayPal.[70]

A secure authentication protocol would allow the federal government to use broadband to deliver a greater set of government services online to the American people,[71] but efforts to improve authentication are limited. Even the ICAM Roadmap offers minimal guidance because it focuses primarily on secure authentication as a cybersecurity issue. The Roadmap says little about services for the public and provides no metrics for measuring the delivery of services.

To address these gaps, OMB and the Federal CIO Council should take the lead in developing a flexible, secure government-wide authentication protocol that covers all levels of identity assurance, from the most secure to the least, and that facilitates the deployment of the next generation of online government services. There is support for a federated scheme with OMB and the Federal CIO Council setting standards.[72] The Federal CIO Council should also revise the ICAM Roadmap to include performance metrics related to government delivery of services to the public.

RECOMMENDATION 14.16: The Executive Branch should establish MyPersonalData.gov as a mechanism that allows citizens to request their personal data held by government agencies.

The federal government holds data on many of its citizens, and the Privacy Act contains provisions for giving people access to it and letting them correct it.[73] As currently implemented, this is a manual and costly process, and it is not easy for citizens to get access to their information online. Were citizens able to securely authenticate their identity online, they could easily verify the information (and correct any errors), thereby increasing its value.[74] Therefore, the Executive Branch should create and maintain MyPersonalData.gov. This tool and corresponding website would serve as an interface so citizens could access the data about them held by federal agencies.

For example, MyPersonalData.gov could allow taxpayers to create tax returns by importing data submitted to the Internal Revenue Service by employers and financial institutions into tax forms. This would save individuals time and money in the preparation of their taxes.[75]

RECOMMENDATION 14.17: Congress should consider re-examining the Privacy Act to facilitate the delivery of online government services and to account for changes in technology.

The Privacy Act is the legal framework for how the federal government handles personal data and information, but it does not address how private third parties handle personal data and information. Its limitations in dealing with the issues that arise with data in electronic databases are well-recognized.[76]

The Privacy Act also provides no guidance on new technologies that have privacy implications, such as the use of persistent cookies on websites.[77] Congressional changes to the

Act could allow agencies to significantly reduce the administrative burden on students applying for financial aid if agencies are allowed to share personal information with each other given appropriate privacy safeguards such as the permission of the person securely authenticated online.

RECOMMENDATION 14.18: The federal government should undertake a series of efforts to improve the delivery of government services online.

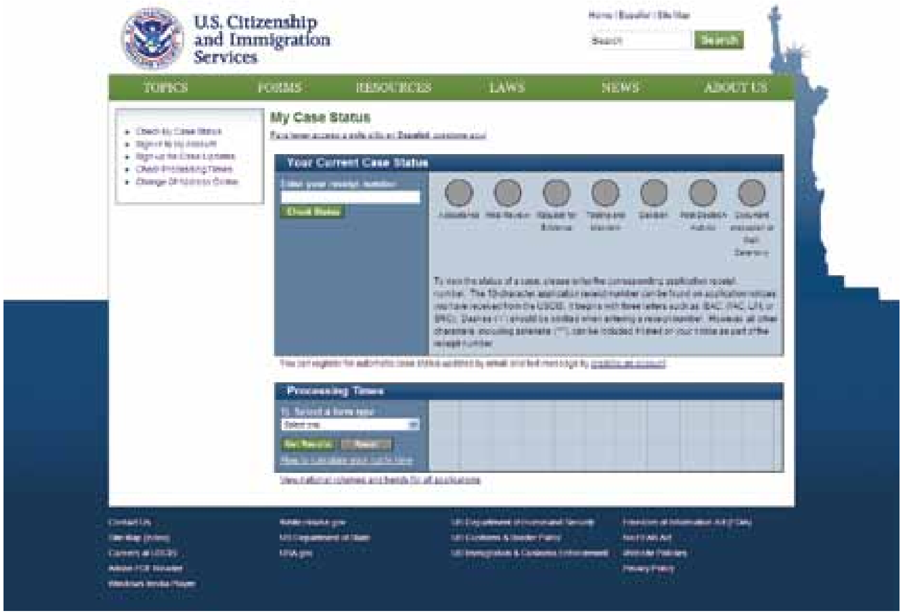
- **OMB should benchmark federal government websites against the private sector and hold agencies accountable for making improvements on an annual basis.**
- **OMB should modernize the Advance Planning Document (APD) process to encourage state governments to develop enterprise-wide solutions.**
- **The Federal Web Managers Council should promulgate Web standards and templates to make the federal Web presence easier to navigate, easier to recognize and accessible to people with disabilities.**
- **OMB should deploy a portion of the E-Government Fund to facilitate replication of leading best practices.**
- **The results of these efforts should be included in OMB's annual E-Government Report to Congress.**

Though some government websites show great promise, many are still built from a siloed, agency-centric perspective, with insufficient focus on developing websites and portals that are integrated, user-friendly and consumer-centric. Though more than 75% of Internet users have visited a government website,[78] reports consistently show that public sector websites lag the private sector.[79] Additionally, the government has failed to meaningfully integrate lessons learned from best practices of leading online government services into its operations. Notable exceptions include the new U.S. Citizenship and Immigration Services (USCIS) portal, which allows applicants to check their immigration status instantly along with typical wait times,[80] and the Open Government Initiative (see Exhibit 14-A and Box 14-2).[81] At the state and local government level, the eCityGov Alliance, comprised of nine cities in the state of Washington, is a successful effort to share best practices and offer cross-government online services.[82] The problem is that the successes are isolated. Not enough has been done to share lessons learned so that other efforts can benefit from the successes.

Sharing best practices can particularly improve the provision of benefits for low-income individuals by state governments. Millions of federal dollars are spent annually on IT that supports these services, and the APD process allows states to obtain approval for the portion of the costs of acquiring new online systems that the federal government contributes. The current system contains important mechanisms to hold states accountable for making smart choices about what systems are developed, but it may also encourage siloed systems, which might add greater costs for later integration as well as biasing states against migrating to solutions that could be more cost-effective in the long term. To address this gap, OMB should work with relevant agencies to modernize the APD process to encourage governments to develop enterprise-wide solutions.

Because public sector websites lag the private sector in usability and design, the Federal Web Managers Council should

Exhibit 14-A:
The U.S. Citizenship and Immigration Services Dashboard



BOX 14-2:

U.S. Citizenship and Immigration Services Offers Online Access

Until recently, when an individual filed an application for citizenship with the U.S. Citizenship and Immigration Services (USCIS), the applicant had no knowledge of his case status. USCIS has recently revamped its website to allow applicants to use an identifying number and immediately check a case status online. Applicants can receive alerts about changes in status via text message and e-mail updates. Most importantly from the applicant's perspective, the whole system is more transparent because wait times and changes in status are clearly documented.

benchmark the design and usability of government websites against leading industry best practices.

OMB should continually recommend specific improvements that agencies should make, highlight best practices in its annual E-Government Report to Congress and deploy the E-Government Fund to help replicate best practices across the federal government.

RECOMMENDATION 14.19: The Executive Branch's review of the Paperwork Reduction Act should aim to enable government to solicit input to improve government services.

The Paperwork Reduction Act is a barrier to implementing many best practices.[83] For example, the Act precludes surveying Web users to improve an agency's Web presence without undertaking an onerous survey-approval process that could take months. One federal employee commented, "[The Paperwork Reduction Act] imposes a burden to obtain any user-generated input … The result is that we often don't go to the trouble."[84] The director of USA.gov, the online gateway to the federal government, has stated that the Act needs to be reexamined for the new media world.[85]

The Executive Branch has begun work on updating the 15-year-old Paperwork Reduction Act.[86] This review should aim to enable the government to engage in a two-way conversation with the public.

RECOMMENDATION 14.20: TheWhite House Office of Science and Technology Policy (OSTP) should develop a five-year strategic plan for online service delivery.

Since the release of the Quicksilver plan for deployment of 24 Presidential-level E-Government initiatives in 2002,[87] there has been no subsequent government-wide effort to develop a strategic plan for online federal government services. OMB currently submits an annual E-Government Report to Congress pursuant to the E-Government Act,[88] but this is an historical summary, not a forward-looking strategic vision.

It is clear that Americans want the opportunity to conduct simple transactions with the federal government online.[89] OSTP should develop a strategic plan, updated every two years, that addresses issues such as accessibility (including issues raised in the Attorney General's biennial report on Section 508 compliance), benefits administration, alternative platforms, and state and local government partnerships.

RECOMMENDATION 14.21: The federal government should improve the delivery of means-tested benefits to low-income Americans.

- **OMB should enhance Partner4Solutions.gov, a platform for improving service delivery of government means-tested benefits, to include a database of government, non-profit and private tools.**
- **OMB should convene a summit in 2010 of state government CIOs, local health and human services leaders and technology innovators to focus on using technology to modernize benefit services.**

Integrating and streamlining processes through the use of broadband can help low-income Americans receive all the safety-net benefits for which they qualify, demonstrably bettering their chances of getting out of poverty. A 2002 Urban Institute report found that getting access to both Supplemental Nutrition Assistance Program benefits (or food stamps) and Medicaid increases the likelihood of job retention for those leaving TANF. Twenty percent of former recipients who secured both benefits returned to welfare, compared with 51% of those who did not secure both benefits. In our current system, many poor people do not receive all the benefits they need or for which they are eligible. Just over half of those eligible for food stamps receive them. Two-thirds of those eligible for Medicaid or the State Children's Health Insurance Program receive it. One-third of those eligible for TANF receive these benefits. Many cite confusion over eligibility and difficulty of application as major barriers.[90]

Many states have started to experiment with a continuum of changes that leverage the Internet. ACCESS NYC uses online calculators that screen residents for 35 benefits in seven languages. Other states have set up "one-stop" online applications for multiple sets of benefits. Still others have gone to large-scale systems integration. Moving toward a modernized, integrated online benefits system would improve service delivery, reduce access barriers and drive efficiency.

A recently-launched federal program, the Partnership Fund for Program Integrity, has begun helping state and local governments find innovative ways to improve benefits programs. It should be used to encourage the move to "one-stops" for online applications. Instead of merely aggregating application forms that will ultimately need to be printed, grantees should move toward electronic signatures, full electronic submission and pre-population of fields based on applications for other benefits, which would save clients time and agencies money. These systems could potentially include secure document imaging and storage. A 2007 GAO report notes that Florida's document management and imaging system lets caseworkers retrieve electronic case records in seconds, compared with as long as 24 hours for paper case files.[91]

Partner4Solutions.gov is a platform for improving service delivery in this space. It should develop a database of online benefits tools from state, local governments and non-profits, functioning as an Apps.gov of the benefits world. Where applicable, the database should include prices (because they can vary so widely). For example, the cost of purchasing or developing a pre-screening tool—an online set of questions to give families a sense of the range and amount of benefits for which they are eligible—costs $15,000 to $5 million.[92]

Finally, numerous state and local governments are working on initiatives to utilize broadband and online service delivery to improve the administration of benefits programs. Although many best practices are being developed, these efforts are occurring independently of each other. To address this gap, OMB should convene a summit in 2010 of state government CIOs, local health and human services leaders, and technology innovators so they can focus on using technology to modernize benefit services. This summit would have three goals: to develop a shared time horizon for moving toward integrated online platforms for key programs for low-income Americans; to showcase and share available data on costs and benefits of current state tools as well as external innovations such as the Annie E. Casey Foundations' Casebook, a Web 2.0 tool for child welfare case management; and to develop a shared set of best practices that states can use to improve service delivery.

CHAPTER 14 ENDNOTES

1 Jason Baumgarten & Michael Chui, *E-Government 2.0*, McKinsey on Gov't, Summer 2009, at 26–27, *available at* http://www.mckinsey.com/clientservice/publicsector/pdf/TG_MoG_Issue4_egov.pdf.

2 Shelley Waters-Boots, Ford Found. et al., Improving Access to Public Benefits: Helping Individuals and Families get the Income Supports They Need (2010), *available at* http://www.opportunityatwork.org/pdf/Improving_Access_To_Public_Benefits_1_12_10.pdf.

3 *See* Jane Patterson, Executive Director, e-NC Authority, State of North Carolina, Remarks at the FCC State and Local Government Workshop (Sept. 1, 2009), *available at* http://www.broadband.gov/docs/ws_19_state_and_local.pdf; John Conley, Deputy State Chief Information Officer, State of Colorado, Remarks at FCC State and Local Government Workshop (Sept. 1, 2009), *available at* http://www.broadband.gov/docs/ws_19_state_and_local.pdf; Gary Gordier, Chief Information Officer and IT Director, El Paso, TX, Remarks at the FCC State and Local Government Workshop (Sept. 1, 2009), *available at* http://www.broadband.gov/docs/ws_19_state_and_local.pdf; FiberTower Comments in re National Broadband Plan NOI, filed June 8, 2009, at 2, 6.

4 Transportation, Treasury, Independent Agencies, and General Government Appropriations Act of 2005, Pub. L. No. 108-447, Div. H, 118 Stat. 2809 (2004).

5 Memorandum from Joshua B. Bolten, Director, Office of Mgmt. & Budget (OMB), to Heads of Departments and Agencies, Regulation on Maintaining Telecommunication Services During a Crisis or Emergency in Federally-owned Buildings, M-05-16 (June 30, 2005), *available at* http://www.whitehouse.gov/omb/assets/omb/memoranda/fy2005/m05-16.pdf; Memorandum from Clay Johnson III, Deputy Director for Management, OMB, to Heads of Departments and Agencies, Implementation of Trusted Internet Connections (TIC), M-08-05 (Nov. 20, 2007), *available at* http://www.whitehouse.gov/omb/assets/omb/memoranda/fy2008/m08-05.pdf; Nat'l Commc'ns Sys., Dep't of Homeland Security, The National Communications System Directive (NCSD) 3-10, Minimum Requirements for Continuity Communications Capabilities (July 25, 2007).

6 E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899 (2002).

7 *See* Alaska Dep't of Educ. Comments in re NBP PN #15 (*Comment Sought on Broadband Needs in Education, Including Change to E-rate Program to Improve Broadband Deployment—NBP Public Notice #15*, GN Docket Nos. 09-47, 09-51, 09-137, CC Docket No. 02-6, WC Docket No. 05-195, Public Notice, 24 FCC Rcd 13560 (WCB 2009) (*NBP PN #15*)), filed Nov. 20, 2009, at 79; State E-Rate Coordinators Alliance Comments in re NBP PN #15, filed Nov. 20, 2009, at 19–20; Am. Ass'n of Sch. Adm'rs & Ass'n of Educ. Serv. Agencies Comments in re NBP PN #15, filed Nov. 20, 2009, at 5–6; Nat'l Ass'n of Telecomm. Officers & Advisors (NATOA) Comments in re NBP PN #15, filed Nov. 20, 2009, at 11–12; AT&T Comments in re NBP PN #15, filed Nov. 20, 2009, at 8–9; City of Chicago Comments in re NBP PN #15, filed Nov. 20, 2009, at 26; Dell Comments in re NBP PN #15, filed Nov. 20, 2009, at 4; Mich. Dep't of Educ. Comments in re NBP PN #15, filed Nov. 20, 2009, at 7; Tex. Educ. Telecomm. Network Comments in re NBP PN #15, filed Nov. 20, 2009, at 3–4; Ohio Pub. Library Info. Network Comments in re NBP PN #15, filed Nov. 17, 2009, at 1–2; Alaska E-Rate Coordinator Comments in re National Broadband Plan NOI, filed June 8, 2009, at 10; U.S. R&E Networks and HIMSS Reply in re NBP PN #30 (*Reply Comments Sought in Support of National Broadband Plan*, GN Docket Nos. 09-47, 09-51, 09-137, Public Notice, 25 FCC Rcd 2417 (WCB 2010) (*NBP PN #30*)), filed Jan. 28, 2010, at 43–44.

8 *See* Alaska Dep't of Educ. Comments in re NBP PN #15, filed Nov. 20, 2009, at 7.

9 IBM, Smarter Cities, http://www.ibm.com/smarterplanet/us/en/sustainable_cities/ideas/ *(last visited Feb. 17, 2010)*; Steve Lohr, *To Do More With Less, Governments Go Digital*, N.Y. Times, Oct. 10, 2009, http://www.nytimes.com/2009/10/11/business/11unboxed.html.

10 Cisco, Literature: Cisco Connected Communities for State and Local Governments, http://www.cisco.com/web/strategy/government/local_connected_communities.html (last visited Feb. 17, 2010).

11 Richard Whitt, *Experimenting with New Ways to Make Broadband Better, Faster, and More Available*, Google Pub. Pol'y Blog, Feb. 10, 2010, http://googlepublicpolicy.blogspot.com/2010/02/experimenting-with-new-ways-to-make.html.

12 Benton Found. Comments in re NBP PN#22 (*Comment Sought on Research Necessary for Broadband Leadership—NBP Public Notice #22*, GN Docket Nos. 09-47, 09-51, 09-137, Public Notice, 24 FCC Rcd 138207 (WCB 2009) (*NBP PN #22*)), filed Dec. 8, 2009, at 9–11; Free Press Reply in re NBP PN #30, filed Jan. 27, 2010, at 13.

13 Pew Res. Ctr. for the People and the Press, Trends in Political Values and Core Attitudes: 1987–2007, at 49 (2007), http://people-press.org/reports/pdf/312.pdf.

14 Ctr. for Digital Gov't, Renovation Nation: Improving Government Service Delivery in Smart and Sustainable Ways 10 (2009), *available at* http://www.govtechblogs.com/fastgov/CDG09RenovationNation.pdf.

15 The National Institute for Standards and Technology (NIST) defines cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." National Institute of Standards and Technology, Cloud Computing, The NIST Definition of Cloud Computing (2009), http://csrc.nist.gov/groups/SNS/cloud-computing/ (last visited Feb. 17, 2010). While there is not universal agreement on the definition, this plan will use the NIST definition. For a full discussion of the definition of cloud computing, see AT&T Comments in re NBP PN #21 (*Comment Sought on Data Portability and Its Relationship to Broadband—NBP Public Notice #21*, GN Docket Nos. 09-47, 09-51, 09-137, Public Notice, 24 FCC Rcd 13816 (WCB 2009) (*NBP PN #21*)), filed Dec. 9, 2009, at 3–5; DataPortability Project Comments in re NBP PN #21, filed Dec. 9, 2009, at 5; FTC Comments in re NBP PN #21, filed Dec. 9, 2009, at 1–2; InCommon Steering Committee Comments in re NBP PN #21, filed Dec. 9, 2009, at 4; Qwest Comments in re NBP PN #21, filed Dec. 9, 2009, at 2–4; Letter from Paula Boyd, Regulatory Counsel, Microsoft, to Marlene H. Dortch, Secretary, FCC, GN Docket No. 09–51 (Jan. 20, 2010) (Microsoft Jan. 20, 2010 *Ex Parte*), Attach. 2 (B. Smith) at 1.

16 Gwen Morton & Ted Alford, Booz Allen Hamilton, The Economics of Cloud Computing 1 (2009) (Morton & Alford, The Economics of Cloud Computing), *available at* http://www.boozallen.com/media/file/Economics-of-Cloud-Computing.pdf.

17 Jason Miller, *Data Center Proliferation Must End, Kundra Says*, Fed. News Radio, Oct. 28, 2009, http://www.federalnewsradio.com/?sid=1796664&nid=263.

18 Morton & Alford, The Economics of Cloud Computing at 5, 9.

19 C.G. Lynch, *How Vivek Kundra Fought Government Waste One Google App at a Time*, CIO.com, Sept. 22, 2008, http://www.cio.com/article/450636/How_Vivek_Kundra_Fought_Government_Waste_One_Google_App_At_a_Time_.

20 Gautham Nagesh, *OPM Claims Victory in Huge e-Payroll System Consolidation*, NextGov, Oct. 21, 2009, http://www.nextgov.com/nextgov/ng_20091021_4165.php.

21 *See* GSA, IT Schedule 70: Maximizing the Speed and Value of IT Acquisition Solutions (2007), *available at* http://www.gsaadvantage.gov/images/products/elib/pdf_files/70.pdf.

22 Patrick Thibodeau, *CIA Endorses Cloud Computing, But Only Internally*, ComputerWorld, Oct. 7, 2009, http://www.computerworld.com/s/article/9139016/CIA_endorses_cloud_computing_but_only_internally.

23 Elise Castelli, *DISA Expands Cloud Computing Services*, Fed. Times, Oct. 5, 2009, http://www.federaltimes.com/article/20091005/IT03/910050304/1036/IT.

24 MeriTalk & Merlin Federal Cloud Initiative, The 2009 Cloud Consensus Report 10 (2009), *available at* http://www.meritalk.com/2009-cloud-consensus.php (must register to download); David Talbot, *Security in the Ether*, MIT Tech. Rev., Jan./Feb. 2010, *available at* http://www.technologyreview.com/web/24166/page1/; Letter from Paula Boyd, Regulatory Counsel, Microsoft Corp., to Marlene H. Dortch, Secretary, FCC, GN Docket Nos. 09-47, 09-51, 09-137 (Nov. 12, 2009) (Microsoft Nov. 12, 2009 *Ex Parte*) at 8; InCommon Steering Committee Comments in re NBP PN #21, filed Dec. 9, 2009, at 5; FTC Staff Comments in re NBP PN #21, filed Dec. 9, 2009, at 2; DataPortability Project in re NBP PN #21, filed Dec. 9, 2009 at 6 (filed as Elias Bizannes); Miguel Helft, *Now, Even the Government Has an App Store*, N.Y. Times, Sept. 15, 2009, http://bits.blogs.nytimes.com/2009/09/15/now-even-the-government-has-an-app-store/; OnLive Reply in re National Broadband Plan NOI, filed July 21, 2009, at 4; Yaana Reply in re National Broadband Plan NOI, filed July 21, 2009, at 4.

CHAPTER 14 ENDNOTES

25 The Federal CIO Council was created by Executive Order 13011 on July 16, 1996. *See* Exec. Order No. 13011, 61 Fed. Reg. 37657 (July 16, 1996). This order was subsequently revoked. *See* Exec. Order No. 13403, 71 Fed. Reg. 28543 (May 12, 2006). The Council's existence was codified by the E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899 (2002) (codified at 44 U.S.C. § 101).

26 Aliya Sternstein, *Feds Offer 38,484 Budget Cuts*, NextGov, Oct. 19, 2009, http://techinsider.nextgov.com/2009/10/feds_offer_38484_budget_cuts.php; OMB, SAVE Award, http://www.saveaward.gov (last visited Feb. 20. 2010).

27 Jason Miller, *Idea to Reuse Medication at VA Hospitals Wins SAVE Award*, Fed. News Radio, Dec. 11, 2009, http://www.federalnewsradio.com/index.php?nid=110&sid=1837851.

28 Memorandum from Peter Orszag, Director, OMB, to the Heads of Departments and Agencies Responding to General Government Proposals from the President's SAVE Award, M-10-09 (Dec. 21, 2009), *available at* http://www.whitehouse.gov/omb/assets/memoranda_2010/m10-09.pdf.

29 OMB, USASpending.gov., http://www.usaspending.gov/faads/tables.php?tabtype=t1&subtype=atf&rowtype=a (last visited Feb. 20, 2010).

30 Jason Miller, *OMB Calls for a Review of Grant Application Systems* (Federal News Radio broadcast March 11, 2009), *available at* http://www.federalnewsradio.com/index.php?nid=35&sid=1621782.

31 Larry Freed, Foresee Results, E-Government Satisfaction Index 2, 6, 18 (2009), *available at* http://www.foreseeresults.com/_downloads/acsicommentary/ACSI_EGov_Report_Q1_2009.pdf.

32 GAO, Grants.gov Has Systemic Weaknesses That Require Attention 5, 24, GAO-09-589 (2009), *available at* http://www.gao.gov/new.items/d09589.pdf.

33 As used here, social media refers to the use of applications within government to facilitate collaboration and information sharing within the federal workforce. See Chapter 15: Civic Engagement for further discussion of the use of social media in government.

34 Jennifer L. Dorn, *Rebooting the Public Square*, Fed. Computer Wk., Dec. 3, 2007, at 30, *available at* http://fcw.com/articles/2007/11/30/web-20-rebooting-the-public-square.aspx?sc_lang=en.

35 Nora Ganim Barnes & Eric Mattson, Ctr. for Marketing Res., Social Media in the 2009 Inc. 500: New Tools & New Trends (2009), *available at* http://www.umassd.edu/cmr/studiesresearch/socialmedia2009.pdf.

36 Ben Bain, *4 Studies in Collaboration—Case 2: TSA's IdeaFactory*, Fed. Computer Wk., Feb. 29, 2008, *available at* http://fcw.com/articles/2008/02/29/4-studies-in-collaboration-151-case-2-tsa146s-ideafactory.aspx; The White House, IdeaFactory, http://www.whitehouse.gov/open/innovations/IdeaFactory/ (last visited Feb. 20, 2010).

37 The White House, IdeaFactory, http://www.whitehouse.gov/open/innovations/IdeaFactory/ (last visited Feb. 20, 2010).

38 Jill R. Aitoro, *Defense More Likely Than Civilian Agencies To Use Social Networking Tools*, NextGov, Jan. 15, 2010, http://www.nextgov.com/nextgov/ng_20100115_4048.php?oref=mostread.

39 *See* Andrea Di Maio, Gartner, Inc., Citizen-Driven Government Must Be Employee-Centric, Too (2009), *available at* http://www.gartner.com/DisplayDocument?doc_cd=168334 (purchase required); Fed. Web Managers Council, Social Media and the Federal Government: Perceived and Real Barriers and Potential Solutions 2 (2008), *available at* http://www.usa.gov/webcontent/documents/SocialMediaFed%20Govt_BarriersPotentialSolutions.pdf.

40 Fed. Chief Info. Officers Council, Guidelines for Secure Use of Social Media by Federal Departments and Agencies 9 (2009), *available at* http://www.cio.gov/Documents/Guidelines_for_Secure_Use_Social_Media_v01-0.pdf.

41 Massimo Calabresi, *Wikipedia for Spies: The CIA Discovers Web 2.0*, Time, Apr. 8, 2009 (Calabresi, *Wikipedia for Spies*), http://www.time.com/time/nation/article/0,8599,1890084,00.html.

42 Calabresi, *Wikipedia for Spies*.

43 Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure Review, iii (2009), *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

44 President's National Security Telecommunications Advisory Committee, Cybersecurity Collaboration Report: Strengthening Government and Private Sector Collaboration Through a Cyber Incident Detection, Prevention, Mitigation, and Response Capability 4 (2009) (Advisory Committee Cybersecurity Collaboration Report), *available at* http://www.ncs.gov/nstac/reports/2009/NSTAC%20CCTF%20Report.pdf.

45 Ellen Nakashima, *More Than 75,000 Computer Systems Hacked in One of Largest Cyber Attacks, Security Firm Says*, Wash. Post, Feb. 18, 2010 (Nakashima, *More Than 75,000 Computer Systems Hacked*), http://www.washingtonpost.com/wp-dyn/content/article/2010/02/17/AR2010021705816.html.

46 Ellen Nakashima, *War Game Reveals U.S. Lacks Cyber-Crisis Skills*, Wash. Post, Feb. 17, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/02/16/AR2010021605762.html.

47 Nakashima, *More Than 75,000 Computer Systems Hacked*.

48 David Drummond, *A New Approach to China*, Official Google Blog, Jan. 12, 2010, http://googleblog.blogspot.com/2010/01/new-approach-to-china.html.

49 Mark Clayton, *US Oil Industry Hit by Cyberattacks: Was China Involved?*, Christian Sci. Monitor, Jan. 25, 2010, *available at* http://www.csmonitor.com/USA/2010/0125/US-oil-industry-hit-by-cyberattacks-Was-China-involved.

50 Statement of Liesyl I. Franz, Vice President, TechAmerica, before *the Subcommittee on Research and Science Education, House Committee on Science and Technology*, 111th Cong. (June 10, 2009), *available at* http://democrats.science.house.gov/Media/file/Commdocs/hearings/2009/Research/10jun/Franz_Testimony.pdf.

51 Statement of Dr. Fred B. Schneider, Samuel B. Eckert Professor of Computer Science, Cornell University), before *the Subcommittee on Research and Science Education, House Committee on Science and Technology*, 111th Cong. (June 10, 2009) *available at* http://democrats.science.house.gov/Media/file/Commdocs/hearings/2009/Research/10jun/Scheider_Testimony.pdf.

52 Ellen Nakashima & John Pomfret, *China Proves to be an Aggressive Foe in Cyberspace*, Wash. Post, Nov. 11, 2009, http://www.washingtonpost.com/wp-dyn/content/article/2009/11/10/AR2009111017588_pf.html (last visited Feb. 19, 2010).

53 Advisory Committee Cybersecurity Collaborative Report at 5.

54 *See* DOJ, International Criminal Investigative Training Assistance Program, http://www.justice.gov/criminal/icitap/ (last visited Feb. 21, 2010).

55 This should include, at a minimum, representatives from the intelligence community, Department of Defense, Department of Justice, Department of Homeland Security, Department of Energy, Department of State, Department of Treasury, Department of Education, Department of Commerce, the Federal Communications Commission, and the Federal Trade Commission.

56 FCC, Connecting the Globe: A Regulator's Guide to Building a Global Information Community, http://www.fcc.gov/connectglobe/ (last visited Feb. 21, 2010).

57 Comcast, *Comcast Launches Comprehensive Internet Security Solution to Help Keep Customers Safe Online* (press release), Aug. 16, 2005, http://www.comcast.com/About/PressRelease/PressReleaseDetail.ashx?PRID=132.

58 Comcast, *Comcast Unveils Comprehensive "Constant Guard" Internet Security Program* (press release), Oct. 8, 2009, http://www.comcast.com/About/PressRelease/PressReleaseDetail.ashx?PRID=926.

59 Dan Goodin, *Anti-virus Protection Gets Worse: What Is This Thing You Call Heuristics?*, Channel Reg., Dec. 21, 2007, http://www.channelregister.co.uk/2007/12/21/dwindling_antivirus_protection/ (last visited Feb. 18, 2010).

60 Alex Goldman, *Top 23 U.S. ISPs by Subscriber: Q3 2008*, ISP Planet, Dec. 2, 2008, http://www.isp-planet.com/research/rankings/usa.html.

61 GAO, Information Security: Progress Reported, But Weaknesses at Federal Agencies Persist, GAO-08-571T (Mar. 12, 2008), *available at* http://www.gao.gov/new.items/d08571t.pdf; *see* Carolyn Duffy Marsan, *GAO: Common Desktop Configuration Holds Promise for Better Security*, Fed. Computer Wk., Mar. 13, 2008 (Duffy, *GAO: Common Desktop Configuration Holds Promise*), *available at* http://fcw.com/Articles/2008/03/13/GAO-Common-desktop-configuration-holds-promise-for-better-security.aspx.

62 Carolyn Duffy Marsan, *U.S. Internet Security Plan Revamped*, Network World, Feb. 11, 2010, http://www.networkworld.com/news/2010/021110-cybersecurity-defense-revamped.html, *see* Duffy, *GAO: Common Desktop Configuration Holds Promise*.

CHAPTER 14 ENDNOTES

63 Judi Hasson, *Agencies Must Submit FISMA Reports Online*, Fierce Gov't IT, Aug. 25, 2009, http://www.fiercegovernmentit.com/story/agencies-must-submit-fisma-reports-online/2009-08-25; Vivek Kundra et al., *Moving Beyond Compliance: The Status Quo Is No Longer Acceptable*, IT Dashboard Blog, Sept. 28, 2009, http://it.usaspending.gov/?q=content/blog&pageno=2.

64 Connected Nation Reply in re NBP PN #30, filed Jan. 27, 2010, at 16–17.

65 GAO, Means-Tested Programs: Determining Financial Eligibility is Cumbersome and Can Be Simplified 3 (2001), *available at* http://www.gao.gov/new.items/d0258.pdf.

66 Fed. Chief Info. Officers Council, Federal Identity, Credential, and Access Management (FICAM), Roadmap and Implementation Guidance (2009), *available at* http://www.idmanagement.gov/documents/FICAM_Roadmap_Implementation_Guidance.pdf.

67 IDManagement.gov, Open ID solutions for Open Government, http://www.idmanagement.gov/drilldown.cfm?action=openID_openGOV (last visited Feb. 20, 2010).

68 Assurance levels indicate the level of confidence in a user's identity. Low assurance level applications might include a customized "My Page" on federal Web sites. Higher assurance level applications might include filing taxes online. For more information, see Memorandum from Joshua B. Bolton, Director, OMB, to the Heads of All Departments and Agencies, E-Authentication Guidance for Federal Agencies, Memo M-04-04, Attach. A (Dec. 16, 2003), *available at* http://www.whitehouse.gov/OMB/memoranda/fy04/m04-04.pdf.

69 This functionality would allow users to save content relevant to them on one page that would be available every time a user signed on.

70 Nat'l Inst. of Health, Open Identity for Open Government at NIH, http://datacenter.cit.nih.gov/interface/interface245/open_gov.html (last visited Feb. 20, 2010).

71 Center for Democracy and Technology Comments in re NBP PN #21, filed on Dec. 9, 2009, at 3 (filed as Heather West); OpenID Foundation Comments in re NBP PN #21, filed Dec. 9, 2009, at 8; AT&T Comments in re NBP PN #29, (*Comment Sought on Privacy Issues Raised by the Center for Democracy and Technology—NBP PN #29*, GN Docket Nos. 09-47, 09-51, 09-137, Public Notice, 25 FCC Rcd 244 (2010) (NBP PN #29), filed Jan. 22, 2010, at 5–8; Microsoft Jan. 21, 2010 *Ex Parte* at 1–13.

72 Center for Democracy and Technology Comments in re PN #21, filed on Dec. 9, 2009, at 6 (filed by Heather West).

73 Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (1974) (codified at 5 U.S.C. § 552a).

74 *See* Andrea Di Maio, Gartner, Inc., The Case for Citizen Data Vaults 3, 4 (2009), *available at* http://www.gartner.com/DisplayDocument?id=1031315 (purchase required); DataPortability Project Comments in re NBP PN #21, filed Dec. 9, 2009, at 7.

75 Randall Stross, *Why Can't the IRS Help Fill in the Blanks?*, N.Y. Times, Jan. 23, 2010, http://www.nytimes.com/2010/01/24/business/24digi.htm.

76 *See generally* Info. Sec. and Privacy Advisory Bd., Toward A 21st Century Framework for Federal Government Privacy Policy (2009), *available at* http://csrc.nist.gov/groups/SMA/ispab/documents/correspondence/ispab-report-may2009.pdf; Ctr. for Democracy and Tech., E-Privacy Act Amendments Wiki, http://eprivacyact.org/index.php?title=Welcome (last visited Feb. 20, 2010); Center for Democracy and Technology Comments filed in re NBP PN #29, Jan. 22, 2010, at 12; Microsoft Jan. 21, 2010 *Ex Parte* at 1–13.

77 InCommon Steering Committee Comments in re NBP PN #21, filed Dec. 9, 2009, at 2–3.

78 John Horrigan, *Broadband Adoption and Use in America* 16 exh. 3 (OBI Working Paper No. 1, 2010), *Horrigan, Broadband Adoption and Use in America.*

79 Jason Baumgarten & Michael Chui, *How We Get to E-Government 2.0*, McKinsey Q., July 28, 2009, *available at* http://www.ciozone.com/index.php/Government-IT/How-We-Get-to-E-government-2.0.html; Larry Freed, E-Government Satisfaction Index 6 (2009), *available at* http://fcg.nbc.gov/documents/ACSI-EGov-commentary_Q2-2008.pdf.

80 U.S. Customs and Immigration Services, http://www.uscis.gov (last visited Nov. 27, 2009).

81 U.S. Office of Science and Technology Policy, http://www.whitehouse.gov/open (last visited Nov. 27, 2009).

82 Massimiliano Claps, Case Study: The eCityGov Alliance Provides Cross-County Online Services Portals (2009).

83 Paperwork Reduction Act of 1980, Pub. L. No. 96-511, 94 Stat. 2812 (1980), *codified at* 44 U.S.C. §§ 3501–21.

84 Vivek Kundra & Michael Fitzpatrick, *Enhancing Online Citizen Participation through Policy*, Open Gov't Blog, June 16, 2009, http://www.whitehouse.gov/blog/Enhancing-Online-Citizen-Participation-Through-Policy.

85 Aliya Sternstein, *Government Seeks to Update Paperwork Rule*, NextGov, Oct. 26, 2009 (Sternstein, *Government Seeks to Update Paperwork Rule*), http://www.nextgov.com/nextgov/ng_20091026_1611.php.

86 *See* Sternstein, *Government Seeks to Update Paperwork Rule*; *see also* Improving Implementation of the Paperwork Reduction Act, 74 Fed. Reg. 55269 (proposed Oct. 27, 2009), *available at* http://www.whitehouse.gov/omb/assets/fedreg_2010/10272009_pra.pdf.

87 *See* OMB, The President's Management Agenda 24 (2002), *available at* http://www.whitehouse.gov/omb/budget/fy2002/mgmt.pdf.

88 E-Government Act of 2002, Pub. L. No 107-347 § 3606, 116 Stat. 2899 44 U.S.C. § 3606 (2002).

89 John Horrigan, *Broadband Adoption and Use in America* (OBI, Working Paper No. 1, 2010).

90 *See, e.g.*, Randy Albelda & Heather Boushey, Ctr. for Econ. & Pol'y Res., Bridging the Gaps: A Picture of How Work Supports *Work* in Ten States 29 (2007), *available at* http://www.bridgingthegaps.org/publications/nationalreport.pdf.

91 GAO, Food Stamp Program: Use of Alternative Methods to Apply for and Maintain Benefits Could be Enhanced by Additional Evaluation and Information on Promising Practices 27, GAO-07-573 (2007), *available at http://* www.gao.gov/cgi-bin/getrpt?GAO-07-573.

92 Sean Coffey et al., Nat'l League of Cities, Screening Tools to Help Families Access Public Benefits 6 (2005), *available at* http://www.nlc.org/ASSETS/E2DF31BA4AFF4ADEB19BA434142B0545/iyefscreeningtools.pdf.