17. INFORMATION TECHNOLOGY

With the radical evolution of technology, the Federal Government has an unprecedented opportunity to accelerate the quality, timeliness, and security of services delivered to the public. In recent years, agency adoption of emerging technologies has had a dramatic impact in efficiency. For example, the United States Digital Service (USDS) supported the United States Citizenship and Immigration Services (USCIS) transition to electronic filings to renew or replace green cards and pay certain immigration fees. Closing down the legacy Electronic Immigration System (ELIS) will save the Department of Homeland Security $33 million a year in ongoing operations, maintenance, and licensing costs. The newly launched myUSCIS makes it easier for users to access information about the immigration process and services. In addition, over the past year major policy milestones were accomplished with the release of government-wide Federal Information Technology Acquisition Reform Act (FITARA) implementation guidance and the launch of the Cybersecurity Strategy Implementation Plan (CSIP) – a sweeping series of actions to continue enhancing the management of information technology (IT) resources and strengthening Federal civilian cybersecurity. The Administration will continue to integrate modern solutions to enhance mission and service delivery by prioritizing four core objectives across the Federal IT portfolio: (1) driving value in Federal IT investments, (2) delivering world-class digital services, to include opening Government data to fuel innovation, (3) protecting Federal IT assets and information, and (4) developing the next generation IT workforce. Highlights of activities and initiatives undertaken to advance these objectives are provided in the Government of the Future chapter in the Budget volume, and in additional detail below.

DRIVING VALUE IN FEDERAL IT INVESTMENTS

Federal Spending on IT—Through a combination of policy guidance and oversight, this Administration has optimized IT spending to save taxpayers money by driving value and cost savings in Federal IT investments, and by delivering better services to American citizens. As shown in Table 17-1, the Budget's total planned spending on IT in 2017 is estimated to be $89.9 billion.[1] Chart 17-1 depicts how 7.1 percent annual growth in IT spending over 2001-2009 has been slowed to 1.8 percent annually for 2009-2017, due in part to the Administration's achievements in improving the efficiency of how funds are spent on IT.

Table 17–1. FEDERAL IT SPENDING
(Millions of dollars)

	2015	2016	2017
Department of Defense	36,727	37,987	38,551
Non-Defense	49,965	50,726	51,300
Total	86,692	88,712	89,850

Note: Defense IT spending includes estimates for IT investments for which details are classified and not reflected on the IT Dashboard. All spending estimates reflect data available as of January 19, 2016.

Focusing Agency IT Oversight on Comprehensive IT Portfolio Reviews—In 2016 and 2017, the Administration will continue to manage Federal IT through the application of PortfolioStat—data driven reviews of agency IT portfolios led by the Office of Management and Budget's (OMB) Office of E-Government and Information Technology (E-Gov). These reviews have evolved each year to ensure Federal IT policy goals are aligned with agency IT portfolios. In addition to assisting agencies with financial savings through reform efforts, PortfolioStat analyzes agency IT investments by using a variety of performance metrics, including whether agencies are delivering their IT investments on budget and on schedule, the use of innovation to meet customer needs, and the protection of Federal data and systems. As part of its ongoing commitment to transparency, the Administration has updated PortfolioStat performance metrics publicly on the IT Dashboard throughout FY 2015, and for the first time will publish continuously updated agency-specific cost savings information.

OMB requires that agency Chief Information Officers (CIOs) rate all major IT investments reflected on the IT Dashboard on a continuous basis and assess how risks for major development efforts are being addressed and mitigated. The IT Dashboard shows continued improvements in the general health of IT investments across government, as denoted by the increased proportion of CIO-rated "Green" investments on the IT Dashboard, which comprised 77 percent of all rated investments in January 2016 compared to 69 percent in 2012 (assessments based on total life cycle of investments).

Implementing FITARA—On December 19, 2014, the President signed FITARA[2], the most comprehensive IT reform law in almost two decades. To aid in government-wide implementation, the Administration released the policy M-15-14: *Management and Oversight of Information Technology*[3] in June. This guidance took major steps toward ensuring agency CIOs have significant involvement in procurement, workforce, and technology-related budget matters. The guidance provides direction on the CIOs' and other Senior Agency Officials' roles and responsibilities

[1] Based on agencies represented on the IT Dashboard, located at: *http://itdashboard.gov*.

[2] See *http://www.gpo.gov/fdsys/pkg/CPRT-113HPRT91496/pdf/CPRT-113HPRT91496.pdf*, page 355.

[3] See *https://www.whitehouse.gov/sites/default/files/omb/memoranda /2015/m-15-14.pdf*

for the management of IT and creates a foundation for lasting partnerships among agency leadership including CIOs, CFOs, CAOs[4] and program leaders to make technology decisions that best support agency missions. It also positions CIOs so that they can be held accountable for how effectively agencies manage the full lifecycle of IT products and services and use modern digital approaches, including agile development, to achieve the objectives of efficient, effective, and secure programs and operations. Over the last year, the Administration has made significant progress in facilitating agency implementation of FITARA and our Common Baseline by requiring agencies to thoroughly review agency implementation plans and integrating FITARA implementation oversight into quarterly PortfolioStat sessions. For example, OMB recently launched a central location for tools and resources to support agencies in implementation, and a dashboard to publicly track agencies' progress.[5] Ensuring full implementation of FITARA remains a top priority in FY 2016 and 2017.

Buying as One—In 2015, the Administration announced the launch of the government-wide Category Management initiative[6] to move the Federal Government toward the goal of buying as one customer. This approach, used extensively by private industry, enables the Federal Government to act more like a single enterprise for a variety of "categories[7]," and the IT category is leader of this new initiative. The Federal Government is the single largest buyer of IT in the world with annual IT contract spending in excess of $50 billion for hardware, software, telecommunications, security, and professional services. Category management has already begun to make significant improvements in IT acquisitions. For example, the first IT Category Management memorandum, M-16-02[8], established policies to prohibit new contracts for laptops and desktops, mandated use of standard configurations, and implemented demand management strategies. The Federal Government has already seen workstation prices from some vendors drop as much as 50 percent. In FY 2017 the Administration will continue to expand Category Management in the areas of hardware, software, telecommunications and services.

Software Reuse and Open Source—In 2016, the Administration will take important steps to improve value to taxpayers when Federal agencies procure software code that has been custom-developed for Federal use. This will enable the brightest minds from around the country to review, improve, and collaborate on Federal Government code, thereby helping to ensure that the code is safe, reliable, and effective in furthering our national objectives.

Government-Wide Successes—The Administration's continued focus on driving value in Federal IT invest-

[4] CFOs are Chief Financial Officers and CAOs are Chief Acquisition Officers.

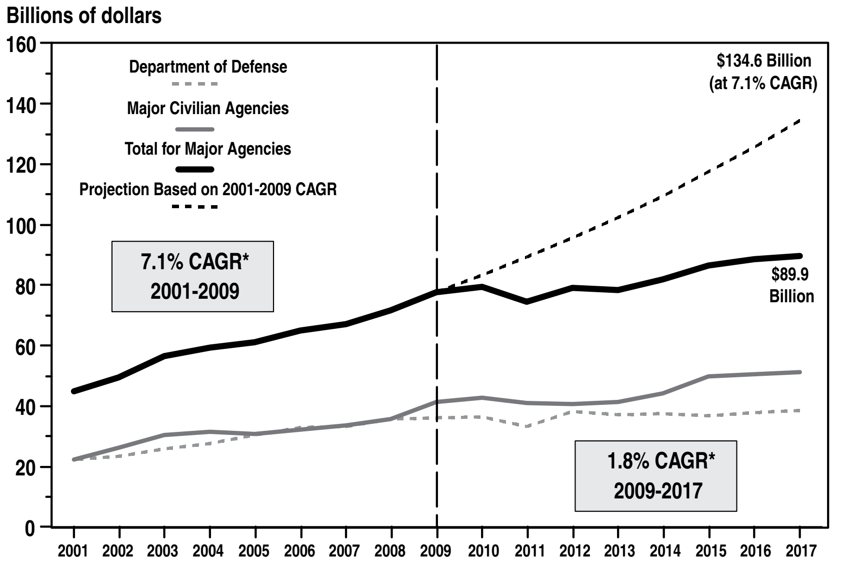
[5] See *https://management.cio.gov*

[6] See *https://www.whitehouse.gov/sites/default/files/omb/procurement/memo/simplifying-federal-procurement-to-improve-performance-drive-innovation-increase-savings.pdf*

[7] Government-wide Category Management includes ten super categories: IT, Professional Services, Security and Protection, Facilities and Construction, Industrial Products and Services, Office Management, Transportation and Logistics Services, Travel and Lodging, Human Capital and Medical. See *https://www.whitehouse.gov/blog/2015/10/14/update-drive-category-management-government-wide* for more detail.

[8] See *https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-02.pdf*

Chart 17-1. Trends in Federal IT Spending



*Compound Annual Growth Rate.

Source: Total IT spending for agencies reporting to the IT Dashboard. Department of Defense has provided estimates for classified IT investments not shown on the IT Dashboard. Chart reflects data available as of January 19, 2016.

ments has led to key successes across the Federal IT portfolio. Specific examples include:

- Government-wide cost savings—Since 2012, the Federal Government has saved over $3.5 billion[9] as a result of the Administration's IT reform efforts, including initiatives such as PortfolioStat, the Federal Cloud Computing Strategy,[10] commodity IT consolidation, migration to shared services, increased use of modern development practices, and data center consolidation and optimization efforts.[11]

- Shifting to more efficient computing services—The Federal Government now spends approximately 8.2 percent of its IT budget on provisioned services such as cloud, on par with leading private sector companies.

- Increased use of modern, agile development practices[12]—Agencies have increased their use of agile development practices and are delivering value 23 days (12 percent) faster since May 2013. Evidence in the IT portfolio shows that these agile projects have been nearly twice as likely to deliver on time as those using "waterfall" development techniques,[13] and have been 33 percent more likely to deliver planned capabilities on budget.[14]

- Data center efforts—As part of the Administration's data center consolidation and optimization efforts, agencies have closed 3,179 data centers as of November 2015, reversing the previous unsustainable data center growth trends, reducing energy consumption and the Federal real estate footprint, and enhancing the Federal IT security posture. The General Services Administration (GSA) leads the Government in data center closures, having closed 88 of its 124 (71 percent) total data centers.

DELIVERING WORLD CLASS DIGITAL SERVICES

Smarter IT Delivery—The Administration has embarked on a comprehensive approach to fundamentally improve the way that the Government delivers technology services to the public. This agenda for the Smarter IT Delivery Cross-Agency Priority (CAP)[15] goal focuses on ensuring that all agencies have access to the best partners, people, and digital practices. As part of this work, top technologists are being recruited to work within agencies on the highest priority projects.

U.S. Digital Service and agency digital service teams—Recruiting the best technologists to work inside of government is a key component of our Smarter IT delivery strategy. The Budget will support the continued recruitment of private sector innovators, entrepreneurs, and engineers to government service. Since 2014, Digital Service Experts recruited into the United States Digital Services (USDS)[16] have worked in collaboration with Federal agencies to implement cutting-edge digital practices on the Nation's highest impact programs, including the continued success and stability of *Healthcare.gov*, the Veterans Benefits Management System, myUSCIS, and the College Scorecard at the Department of Education[17], as well as partnering with the Internal Revenue Service to deliver better online taxpayer services to citizens. The College Scorecard was redesigned with direct input from students, families, and their advisers to provide the clearest, most accessible, and reliable national data on college cost, graduation, debt, and post-college earnings. For the first time the public can access the most reliable and comprehensive data on students' outcomes at specific colleges, including former students' earnings, graduates' student debt, and borrowers' repayment rates. Various organizations are already using this data to provide tools to consumers to help them make better informed financial decisions for themselves and their families[18].

USDS also created a new Rapid Response team. This team's work included supporting *Healthcare.gov* during the 2015 open enrollment season and restoring service for the State Department's Consolidated Consular Database, after an outage led to a two-week suspension of visa issuances worldwide.

Digital Acquisition Efforts—In addition to its delivery efforts, USDS is promoting innovation within government contracting and working to build a more ag-

[9] As reported by agencies. Savings described in this chapter can be recognized in two different ways, as defined in OMB Circular A-131: (a) Cost-Savings: A reduction in actual expenditures below the projected level of costs to achieve a specific objective; and, (b) Cost-Avoidance: An action taken in the immediate timeframe that will decrease costs in the future. For example, an engineering improvement that increases the mean time between failures and thereby decreases operation and maintenance costs is a cost-avoidance action.

[10] See *http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf*

[11] See *http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fdcci-update-memo-07202011.pdf*

[12] Agile development is an incremental, fast-paced style of software development to reduce the risk of failure by getting working software into users' hands quickly by releasing bundles of features in frequent sprints based on evolving user needs. For additional information on the benefits of agile development, see *http://www.whitehouse.gov/sites/default/files/omb/procurement/guidance/modular-approaches-for-information-technology.pdf*.

[13] Waterfall development typically proceeds in sequential phases of consistent, fixed duration to produce a complete system. Such full system development efforts can take several years, potentially resulting in a product that is either outdated by the time it is released or contains features that are not aligned with user needs.

[14] Projects which are "on time" and "on budget" have schedule and cost variance of less than 10 percent and are depicted as "green" on the IT Dashboard.

[15] The mission of the Smarter IT CAP goal is to improve outcomes and customer satisfaction with Federal services through smarter IT delivery and stronger agency accountability for success. For more information on CAP goals, see *http://www.performance.gov*.

[16] See *https://whitehouse.gov/digital/united-states-digital-service*

[17] *https://collegescorecard.ed.gov*

[18] See *https://www.whitehouse.gov/blog/2015/09/12/under-hood-building-new-college-scorecard-students*

ile procurement process. In partnership with the Office of Federal Procurement Policy (OFPP), USDS created and launched the Digital Service Contracting Professional Training and Development Program, which seeks to spur innovation in the training of Contracting Officers. This program challenged companies to develop a program that will teach best practices in the procurement of digital services and the important role Contracting Officers can play in building meaningful, successful services. USDS and OFPP identified the winning training program, and the first class of Contracting Officers enrolled in October of 2015.

Information as an Asset—Government Open Data—Open government data enables private sector innovation, facilitates use, and maximizes the nation's return on its investment in data. Since releasing Executive Order 13642[19] and OMB Memorandum M-13-13[20] in 2013, this Administration has continued to make progress towards its open data commitment. *Data.gov* now features over 200,000 datasets on topics such as education, public safety, health care, energy, and agriculture. To further this progress and to support the federal open data ecosystem, additional resources have been provided and expanded such as Project Open Data[21] which provides tools that enable agencies to make their data publicly available, and the Project Open Data Dashboard[22] which provides the public and relevant stakeholders a quarterly evaluation of agencies' open data progress. To facilitate the usage of open data and to increase public dialogue around open data, eight Federal agencies co-hosted Open Data Roundtables to conduct action-oriented dialogues that connect agencies with the organizations that use their data to help identify high value datasets and establish open data priorities. Going forward, this Administration will continue to increase agency data inventories, improve the discoverability of existing data, and work to reduce open data barriers within agencies.

[19] See *https://www.whitehouse.gov/the-press-office/2013/05/09/executive-order-making-open-and-machine-readable-new-default-government-*

[20] See *https://www.whitehouse.gov/sites/default/files/omb/memoranda/2013/m-13-13.pdf*

[21] See *https://project-open-data.cio.gov*

[22] See *http://labs.data.gov/dashboard/offices*

CYBERSECURITY: PROTECTING FEDERAL IT ASSETS AND INFORMATION

Strengthening the cybersecurity of Federal networks, systems, and data is one of the most important challenges we face as a Nation. As cyber risks have grown in severity over recent years, the Administration has executed a comprehensive strategy to address cybersecurity across the Nation, as outlined in the National Security Chapter. Building upon the Administration's broader efforts for 21st Century Cybersecurity, in 2015 the Office of Management and Budget, in coordination with the National Security Council (NSC), the Department of Homeland Security (DHS), the Department of Commerce, as well as other departments and agencies, executed a series of actions to bolster Federal cybersecurity and secure Federal information systems through the Cybersecurity Strategy and Implementation Plan (CSIP).

In 2015, these actions and others led to areas of significant progress across the Federal Government. Federal civilian agencies took action to patch critical vulnerabilities, identify high-value assets, tightly limit the number of privileged users with access to authorized systems, and dramatically accelerate the use of Personal Identity Verification (PIV) cards or alternative forms of strong authentication for accessing networks and systems. Indeed, since the Cybersecurity Sprint, an intensive effort conducted in July 2015 to assess and improve the health of all Federal assets and networks, both civilian and military, Federal Civilian agencies have nearly doubled their use of strong authentication for all users from 42 percent to 81 percent.

Still, as outlined in the CSIP, challenges remain. The Federal Government has identified three primary challenges:

- Outdated Technology – The Federal Government relies significantly on hard-to-defend legacy hardware, software, applications, and infrastructure, which make it particularly vulnerable to malicious cyber activity, as well as costly to defend and protect.
- Fragmented Governance – Governance and management structures are unable to consistently provide effective, well-coordinated cybersecurity across the Federal Government.
- Workforce Gaps—Workforce shortages and skill gaps, including training, education, and recruitment and retention of cybersecurity and privacy professionals, are significant.

To address these challenges and continue moving the needle on cybersecurity for the Federal Government, the President's 2017 Budget invests over $19 billion, or a 35 percent increase from FY 2016, in overall Federal resources for cybersecurity.

Enhancing Federal IT to Secure Federal Information and Assets

The technology, architectures, and processes underpinning Federal Government operations need to be modernized to improve cybersecurity. Of the $51 billion in Federal civilian IT spending planned for FY 2017, approximately 71 percent ($36 billion) is dedicated to maintaining legacy IT investments. Improving Federal cybersecurity will require an accelerated push to strengthen the Government's highest value IT and information assets and to retire, replace, or upgrade hard-to-defend legacy IT. This will require not just modernizing hardware and software, but also improving how we manage the lifecycle of IT investments so that security gains can be sustained over time. This approach will improve the government's risk management capability, improve the cyber-defense landscape, and enhance our ability to respond to changing threats. Therefore, the Administration is proposing a revolving fund at GSA, seeded with an initial capital injection of $3.1 billion, to retire, replace or upgrade hard-to-secure legacy IT systems and transition to new, more secure, efficient, modern IT systems, while also establishing long-term mechanisms for Federal agencies to regularly refresh their networks and systems based on up-to-date technologies and best practices.

A project review board, comprised of experts in IT acquisition, cybersecurity, and agile development, will review agency business cases and select projects for funding to ensure prioritization of projects with the highest risk profile, government-wide impact, and probability of success. The board will identify opportunities to replace multiple legacy systems with a smaller number of common platforms – something that is difficult for agencies to do when acting on their own with limited insight into other agencies' operations. As a result, the central fund will achieve a far greater and more rapid impact than if the funds were allocated directly to agencies. In addition, a team of systems architects and developers will provide additional oversight and development capabilities to make these major changes. The revolving fund will be self-sustaining by requiring agencies to repay the initial investments through efficiencies gained from modernization, ensuring the fund can continue to support projects well beyond the initial infusion of capital. Seed funding of $3.1 billion would address an estimated $12 billion worth of modernization projects over 10 years.

Finally, the Budget includes $275 million in funding to accelerate implementation of the DHS continuous diagnostics and monitoring (CDM) program. CDM enables agencies to invest in a centralized continuous monitoring program that will allow them to quickly and efficiently identify cybersecurity vulnerabilities and mitigate risk.

Streamlining Governance and Ensuring Effective Oversight

Over the long term, the Federal Government will need to move away from a model of IT and cybersecurity governance where individual departments and agencies build, provision, and manage nearly all aspects of their IT and cybersecurity, from infrastructure to platforms to applications. Instead, IT systems and cybersecurity capabilities will need to be built, acquired, and managed in a more holistic way, one that treats the Federal Government as an enterprise and that relies more on shared platforms and common services. This Budget lays the foundation for shifting to this more effective approach to Federal cybersecurity by supporting investments in common IT solutions for small agencies, more secure, enterprise-wide email systems, and common cybersecurity tools and services. Further, the Federal Government needs to improve not only its hardware and software, but how it acquires technology, so that it can keep up to date with industry best practices and emerging technologies in the future.

Today's sophisticated cyber incidents have also demonstrated the need for more coordinated and nimble Government efforts when they occur. In such instances, the Government may need to play an important coordinating role. Moving forward, the Budget supports Federal Government efforts to continue developing policy and plans that establish a foundation for a scalable, flexible, and cooperative approach to significant cyber incident coordination involving both public and private sector stakeholders, and anchors it within the broader National Preparedness System.

In 2016 and 2017, the Administration, including OMB and NSC staff, will also coordinate with DHS to continue working with agencies to identify and remediate weaknesses in cybersecurity programs while ensuring agency progress towards the Cybersecurity Cross-Agency Priority (CAP) Goal through CyberStat reviews. These reviews provide the opportunity for agencies to identify the cybersecurity areas where they may be facing implementation and organizational challenges.

Strengthening the Cybersecurity Workforce

There is a shortage of skilled cybersecurity experts and privacy professionals throughout the IT industry as a whole, and that shortage is more acute within the Federal Government. The Budget includes $62 million for three initiatives to address this recruitment challenge by:

1. Expanding the National Science Foundation's (NSF) CyberCorps®: Scholarship for Service (SFS) program to establish a sustainable cadre of cyber reservists and enhance opportunities for career cybersecurity experts across departments and agencies that can serve the Federal Government to help rapidly respond to cybersecurity challenges;

2. Developing a foundational cybersecurity curriculum for academic institutions to consult and adopt; and

3. Providing grants to academic institutions to develop or expand cyber education programs as part of the National Centers of Academic Excellence in Cybersecurity Program.

In addition to funding these foundational workforce initiatives, this Budget also invests over $37 million to expand standing teams of cybersecurity experts within DHS to provide readily-available cybersecurity capabilities to departments and agencies.

As malicious cyber activity becomes increasingly sophisticated and persistent in the digital age, so must our actions to tackle it. Cyber threats cannot be eliminated entirely, but they can be managed much more effectively. Through these investments, the Administration continues to lead a broad, strategic effort to combat cyber threats, update and modernize Federal cybersecurity policies and procedures, and strengthen the Federal Government's overall cybersecurity infrastructure through modernization efforts.

To complement these steps and focus on long-term challenges in cybersecurity, the Budget also supports the creation of the first Federal Chief Information Security Officer, and the establishment of a blue ribbon commission consisting of leaders in the fields of cybersecurity, technology, privacy, national security, and government.

This commission will identify recommendations for the President, future Administrations, and the Nation to enhance cybersecurity awareness and protections inside and outside of government and to empower Americans to take better control of their digital security.

DEVELOPING THE NEXT GENERATION IT WORKFORCE

Having a high-caliber IT workforce is key to lasting success in each of the Administration's technology initiatives. For example, the Administration has set an aggressive goal of hiring and placing 500 top technology and design experts to serve in the U.S. Government by January 2017 to dramatically improve customer satisfaction with federal technology services. To aid in this, USDS worked with OPM to create a term-appointment hiring authority for Digital Services Experts to more quickly get talent into government, which is now being used by USDS and Agency Digital Service teams. Individuals hired under this authority may serve up to two years once appointed, meaning staff appointed at the end of 2017 could extend into 2019. Working with OPM to expand flexible hiring options and spread proven hiring practices will remain a focus area in FY 2017.

Additionally, in FY 2017 OMB will continue to build off of existing training opportunities being offered to current Federal IT professionals to scale modern development practices across the workforce. For example, this past year the CIO Council, CAO Council and OMB launched the IT Solutions Challenge. Over several months, more than 40 IT and Acquisition professionals in the GS-9 through GS-13 range worked in teams to develop innovative solutions for some of the biggest challenges in IT and acquisitions. These types of training programs work in tandem with expanding the Government's digital acquisition expertise. In the past year, 30 Federal acquisition professionals piloted an innovative approach to training to improve digital IT acquisition capabilities.

CONCLUSION

Ensuring the efficiency, effectiveness, and security of Federal IT has never been more central to how Americans are served by their Government. Over the past seven years, this Administration has focused on driving efficiencies in the way the Government buys, builds, and delivers IT solutions to provide improved services to citizens, and these efforts will be strengthened in 2016 and further scaled across Government in 2017. The 21st Century digital service delivery standards being set by this Administration represent an important commitment to future generations. The 2017 Budget includes funding that will launch the Nation on a path to hire the leading digital experts, institutionalize modern digital delivery practices, and establish more effective partnerships both within Government and with the private sector that will provide services to our citizens at a historical level of quality and timeliness.