Government Cloud Computing Policies: Potential Opportunities for Advancing Military Biomedical Research

Frank J. Lebeda, PhD; Jeffrey J. Zalatoris, PhD; Julia B. Scheerer, PhD

ABSTRACT Introduction: This position paper summarizes the development and the present status of Department of Defense (DoD) and other government policies and guidances regarding cloud computing services. Due to the heterogeneous and growing biomedical big datasets, cloud computing services offer an opportunity to mitigate the associated storage and analysis requirements. Having on-demand network access to a shared pool of flexible computing resources creates a consolidated system that should reduce potential duplications of effort in military biomedical research. Methods: Interactive, online literature searches were performed with Google, at the Defense Technical Information Center, and at two National Institutes of Health research portfolio information sites. References cited within some of the collected documents also served as literature resources. Results: We gathered, selected, and reviewed DoD and other government cloud computing policies and guidances published from 2009 to 2017. These policies were intended to consolidate computer resources within the government and reduce costs by decreasing the number of federal data centers and by migrating electronic data to cloud systems. Initial White House Office of Management and Budget information technology guidelines were developed for cloud usage, followed by policies and other documents from the DoD, the Defense Health Agency, and the Armed Services. Security standards from the National Institute of Standards and Technology, the Government Services Administration, the DoD, and the Army were also developed. Government Services Administration and DoD Inspectors General monitored cloud usage by the DoD. A 2016 Government Accountability Office report characterized cloud computing as being economical, flexible and fast. A congressionally mandated independent study reported that the DoD was active in offering a wide selection of commercial cloud services in addition to its milCloud system. Our findings from the Department of Health and Human Services indicated that the security infrastructure in cloud services may be more compliant with the Health Insurance Portability and Accountability Act of 1996 regulations than traditional methods. To gauge the DoD's adoption of cloud technologies proposed metrics included cost factors, ease of use, automation, availability, accessibility, security, and policy compliance. Conclusions: Since 2009, plans and policies were developed for the use of cloud technology to help consolidate and reduce the number of data centers which were expected to reduce costs, improve environmental factors, enhance information technology security, and maintain mission support for service members. Cloud technologies were also expected to improve employee efficiency and productivity. Federal cloud computing policies within the last decade also offered increased opportunities to advance military healthcare. It was assumed that these opportunities would benefit consumers of healthcare and health science data by allowing more access to centralized cloud computer facilities to store, analyze, search and share relevant data, to enhance standardization, and to reduce potential duplications of effort. We recommend that cloud computing be considered by DoD biomedical researchers for increasing connectivity, presumably by facilitating communications and data sharing, among the various intra- and extramural laboratories. We also recommend that policies and other guidances be updated to include developing additional metrics that will help stakeholders evaluate the above mentioned assumptions and expectations.

INTRODUCTION

This position paper focuses on cloud computing policies that have been developed by the White House, DoD, Defense Health Agency (DHA), the Services and other Federal agencies to facilitate future advances in military medicine and biomedical research. The drivers of the White House Office of Management and Budget (OMB) Cloud First policy were based on the reduction of costs through consolidating government data centers by moving information technology (IT) services to cloud systems and by saving energy (i.e., lower power requirements; green IT). The Federal Cloud Computing Strategy, which instituted this policy in 2011,[1] used the term cloud computing as defined by the National Institute of Standards and Technology (NIST) (see Methods).[2] Cloud computing was also envisioned to provide agency- or program-specific benefits and to efficiently store, manage, integrate, and share large volumes of biomedical research data.

Along with the development and adoption of federal and agency cloud computing policies and strategies, the complexity and scale of biomedical research are growing rapidly to accelerate the systems-wide interrogation of health and medical conditions.

Systems Biology Collaboration Center, US Army Center for Environmental Health Research, 568 Doughten Drive, US Army Medical Research and Materiel Command (USAMRMC), Fort Detrick, Frederick, MD 21702-5010

doi: 10.1093/milmed/usx114

Health-related information is being collected world-wide in ever-growing heterogeneous data sets, with estimated sizes expanding from petabytes (1 PB ~10^{15} bytes or ~1000 terabytes) in 2012 to exabytes (1 EB ~10^{18} bytes or ~1,000,000 terabytes) by 2020.[3]

To improve the capacity for scientists to store, manage, analyze, and share this substantial amount of data, biomedical researchers and bioinformatics companies are building the requisite search engines and software tools to manipulate and analyze large-scale data in parallel and distributed computing systems such as the cloud.[4] For example, the National Institutes of Health (NIH) Microbiome Cloud Project is a partnership of scientists from NIH, academia, and industry to address health issues starting with sequencing approaches.[5] This cloud-based platform has been developed to collect Human Microbiome Project data on the colonizing bacteria, fungi, and other human-associated microbes along with tools to analyze the large-scale dataset, whose size is presently greater than 11 terabytes.[6] A five-terabyte portion of Human Microbiome Project sequencing data is publicly available on the Amazon Web Services cloud.[7] Besides more collaborations and data sharing, another expected outcome of the Microbiome Cloud Project is to identify best practices for using cloud technologies for biomedical research.[8] In another effort, the Broad Institute of Harvard and MIT is moving the Genome Analysis Toolkit (GATK) to cloud resources for its more than 31,000 registered users.[9] This program runs on a cloud software framework[10] that can support a variety of analytic programs, e.g., DNA analysis pipelines,[11] ligand-based predictive drug discovery models,[12] and analysis of functional magnetic resonance imaging (fMRI) datasets.[13] Additional biomedical research applications, e.g., next-generation sequencing, are also available on other cloud big-data frameworks.[14] These steadily growing "omics" and other big datasets that are, or will be, gathered at different DoD facilities[15] are perhaps the most compelling driver for clinicians, biomedical researchers and other stakeholders for considering cloud solutions.

From a DoD perspective, the previously reported systems biology studies being conducted by US Army Medical Research and Materiel Command (USAMRMC) investigators across seven geographically separated laboratories[16] were limited in their technical ability to easily transfer and share data to form additional project collaborations, despite the existence of a centralized digital data and analytical resource[17]. In contrast, it appears that the "Person-Event Data Environment (PDE) represents a vanguard effort that unifies disparate Army and DoD databases in a secure cloud-based enclave,"[18,19] and it provides a collaborative platform that is primarily for psychological and healthcare studies. The expansion of the PDE is part of a 2017 Army Directive that implements the Human Capital Big Data strategy. This Directive also identifies other potential barriers to the process of transferring data to other organizations, such as being compliant with applicable privacy laws, policies, regulations and statutes.[20] Once data are placed in a cloud system and data transfer/sharing policies and compliance issues are resolved, then DoD biomedical researchers should be encouraged to use cloud services, which is a major aim of the cloud policies being reviewed here. Being in compliance with these cloud policies should also help to initiate collaborative research to solve problems in military medicine.

This paper reviews selected government policies and guidances on cloud computing that have appeared since 2009, including associated assumptions and expectations. Based on the issues discussed, our position is that the DoD biomedical researchers and their extramural collaborators who take advantage of cloud computer services will provide future advances in military medicine and biomedical research.

METHODS

Literature Search Details

Online literature searches were performed with Google, Google Scholar, at the Defense Technical Information Center (DTIC) (http://www.dtic.mil/dtic/), at the NIH with the Research Portfolio Online Reporting Tools (RePORT, https://report.nih.gov/), and with the Federal RePORTer (https://federalreporter.nih.gov/). Examples of query terms include: cloud policy, cloud strategy, cybersecurity, data breach, and distributed computing. The relevant documents retrieved were official memoranda, Directives, Instructions, Public Laws, reports, and other publications. References cited within some of the documents also served as literature resources. These documents were down-selected for inclusion in Table 1 if cloud computing was subjectively considered to be a primary focus. Outputs from the breach portal of the Department of Health and Human Services (DHHS), Office of Civil Rights (https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf) were used in determining the relative number of breaches in Health Plans and other covered entities.[21]

Definitions

The NIST Special Publication 800-145 defined 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."[2] The five essential characteristics of cloud computing identified were "on-demand service, broad network access, resource pooling, rapid elasticity (i.e., expansion), and measured service" (i.e., tracking cloud usage to assess cloud availability).[22] Cloud computing can also be thought of as including different converging technologies, e.g., broadband networks, virtual devices, or resources .

Four different cloud deployment models have also been defined by NIST based on different organizational objectives: Private Cloud, "for an organization that may be managed by that organization or a third party which may exist on- or off-premise; Community Cloud, shared by several organizations that supports a specific community with shared objectives and may be managed by the organizations or a third party and which may exist on- or off-premise; Public Cloud, available to

TABLE I. Timeline of Selected Government Cloud Computing Policies and Other Documents

Year	Agency, and/or Official	Title	Comments
2010	OMB, US CIO[27]	Report: 25 Point Implementation Plan to Reform Federal IT Management	Addresses "25 of the most pressing and persistent Federal IT challenges" and a "Shift to Cloud First policy."
2010	OMB, Federal CIO[28]	Memo: Federal Data Center Consolidation Initiative	The FDCCI "addresses challenges by leveraging and promoting best practices in the public and private sector by reducing the energy and footprint of government data centers; reducing the cost of data center hardware, software and operations; increasing IT security; shifting IT investments to more efficient (cloud) platforms and technologies."
2011	OMB, US CIO[1]	Report: Federal Cloud Computing Strategy	Addresses inefficiencies (e.g., low utilization, duplication) and government service delivery that can be improved with cloud computing.
2011	DoD, CIO[38]	Report: DoD Information Technology (IT) Enterprise Strategy and Roadmap Version 1.0 – 6 SEP 11	"Detailed descriptions, initial implementation timelines, and rough-order-of-magnitude (ROM) estimates of the required investments and potential savings were developed for 26 initiatives." The "Cloud Computing initiative moves computing services into the cloud" to improve information security, reduce infrastructure costs, and enable rapid discovery and use of new net-centric capabilities.
2012	DoD, CIO[36]	Report: DoD Cloud Computing Strategy	"Expands the DoD Cloud Computing Strategy to address use of commercial cloud services."
2012	ASD(HA)[40]	Memo: Military Health System Cloud First Adoption Directive and Policy Guidance	"Applies to any MHS IT organization delivering health services to their respective constituents. The scope of this memorandum includes "any and all plans in process or in execution related to adoption or implementation of cloud computing technologies, services, or virtualization solutions."
2014	NDAA FY2015[88]	Public Law 113-291: Federal Information Technology Acquisition Reform Act (FITARA)	Implements, in general, "a data center consolidation and optimization strategy under this section, a covered agency shall do so in a manner that is consistent with Federal guidelines on cloud computing security."
2014	DoD,CIO[39]	Memo: Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services	DoD components may acquire cloud services directly without using DISA as a cloud broker.
2015	Navy, CIO[49]	Memo: Acquisition and Use of Commercial Cloud Computing Services	Provides updated guidance that is compliant with 2014 DoD memo.[39]
2015	Army, CIO[33]	Report: Army Cloud Computing Strategy v.1.1	"Establishes and communicates the Army's vision and strategy for delivering cloud-enabled network capabilities."
2015	Army, CIO[47]	Memo: Guidance for Migration to, and Use of, Commercial Cloud Service Providers (CSPs)	"Provides an authorized alternative to leverage approved commercial CSPs to satisfy requirements issued by the Under Secretary of the Army,[89] the DoD CIO[39] and the 2015 Army Cloud Computing Strategy."[33]
2016	Secretary of the Army[89]	Army Directive 2016-38: Migration of Army Systems and Applications to Approved Hosting Environments and Consolidation of Data Centers.	Describes an "implementation plan for a range of actions necessary for the Army to rationalize and modernize IT systems and applications, migrates them to approved hosting environments, and close or consolidate data centers." "reduce the number of Army IT systems and applications and optimize those remaining to operate in modern, cloud-enabled computing environments."
2016	Federal CIO[90]	OMB Memo M-16-19: The Data Center Optimization Initiative (DCOI)	"Requires agencies to develop and report on data center strategies to consolidate inefficient infrastructure, optimize existing facilities, improve security posture, achieve cost savings, and transition to more efficient infrastructure, such as cloud services and inter-agency shared services."
2016	GAO[76]	Report: Cloud Computing - Agencies Need to Incorporate Key Practices to Ensure Effective Performance	Recommends that OMB include 10 key service-level agreement practices and that government agencies have these service and performance expectations in their agreements with providers.
2016	GSA[78]	Report: Best Business Practices for USG Cloud Adoption	"Provides an overview of business practices for federal agencies to consider when preparing for a migration to the Cloud."

(continued)

TABLE I. Continued

Year	Agency, and/or Official	Title	Comments
2016	DHA, Director[41]	Memo: Defense Health Agency Use of Cloud Computing and Hosting Services	Requires DHA to "comply with all statutory, regulatory and policy requirements for the acquisition and implementation of any and all cloud computing and hosting services."
2016	DoD IG[87]	Report: DoD Needs an Effective Process to Identify Cloud Computing Service Contracts	"DoD did not maintain a comprehensive list of cloud computing service contracts."
2017	Secretary of the Army[20]	Army Directive 2017-04: Implementation of the Army Human Capital Big Data Strategy	Defines an "overarching human data use policy and expands an existing technology – Person-event Data Environment (PDE) – that integrates data across the human capital enterprise" and "unifies disparate Army and DoD databases in a secure cloud-based enclave."
2017	DoD, DISA[62]	Report: DoD Cloud Computing Security Requirements Guide (SRG)	Outlines "the security model by which DoD will leverage cloud computing with the security controls and requirements for using cloud-based solutions."
2017	DoD CIO[60]	DoD Instruction: Risk Management Framework (RMF) for DoD Information Technology (IT)	"Establishes and uses an integrated enterprise-wide decision structure for cybersecurity risk management (the RMF)." "DoD organizations contracting for external IT services" "must comply with DoD cloud computing" policies and guidance.

the general public or a large industry group and owned by an organization selling cloud services; Hybrid Cloud, composed of private, community, or public clouds to create attractive conditions for data and application sharing."

Potential Source of Error

Some relevant policies and memoranda may not have been found, cited, or analyzed for content because they may not have been posted at public websites at the time of this review.

RESULTS

Cloud Computing: Access and Usage Policies of the Federal Government

Vivek Kundra, the first U.S. Chief Information Officer (CIO),[23] was an early proponent of cloud services who organized a "storefront" website for federal agencies to buy cloud-based IT services to improve their productivity, collaborations, and transparency.[24–26] In 2010, the OMB launched the Federal Data Center Consolidation Initiative (FDCCI) to support "green IT" by reducing energy consumption and the number of government data centers, and thereby reducing associated costs for hardware, software, and operations.[27–30] Indeed, as an early adopter, the Army Experience Center's implementation of cloud computing "cost 1/20 of the estimate to upgrade a legacy system."[31] The FDCCI envisaged the migration from traditional to cloud-based systems in a manner that could be rapidly scaled up (in storage capacity) to help Government become "more transparent, open and participatory."[32]

The OMB issued the Federal Cloud Computing Strategy in 2011 and described the Cloud First policy that was intended to increase the rate at which the Government evaluated cloud services prior to buying new on-premise systems (see Methods, Definitions).[1,33] That year, the OMB[34] stated that cloud computing by the Government could "dramatically reduce procurement and operating costs and greatly increase the efficiency and effectiveness of services provided to its citizens."[35]

Cloud Computing: Access and Usage Policies of the Department of Defense

The Federal Cloud Computing Strategy of 2011[1] prompted federal agencies to develop internal strategies. The DoD's 2012 Cloud Computing Strategy[36] advocated the use of commercial cloud services to foster the adoption of cloud computing, optimize data center consolidation, establish the DoD Enterprise cloud infrastructure, and deliver cloud services. The DoD and its agencies were mandated by the National Defense Authorization Act for Fiscal Year (FY) 2012[37] to develop a strategy to migrate to cloud computing services. In compliance with the Act, the DoD released the "DoD IT Enterprise Strategy and Roadmap"[38] and the "DoD Cloud Computing Strategy."[36] The Defense Information Systems Agency (DISA) was the DoD's sole source authorized to acquire cloud services

until 2014 when DoD Components were allowed to acquire cloud services directly."[39]

In 2012, the Assistant Secretary of Defense for Health Affairs (ASD[HA]) issued the "Military Health System (MHS) Cloud First Adoption Directive and Policy Guidance."[40] The MHS Cloud First guidance was designed to provide "the right information to the right customers at the right time." In continuing to develop cloud computing policies, the Director of DHA issued a memorandum in 2016 regarding the DHA's use of cloud computing and hosting services that would comply with all statutory, regulatory and policy requirements for the acquisition and implementation of cloud computing and hosting services.[41] MHS cloud-based systems will use a health IT (HIT) approach which involves electronic health record (EHR) systems and the electronic sharing of information.[42] The "HIT Research and Development Directory" is an inventory of MHS HIT projects in which the version assembled on 27 April 2017 contains descriptions of current and recently completed cloud-related projects.[43] In addition, future MHS cloud-based systems will include a patient's permanent military EHR along with data derived from the revised Joint Tactical Combat Casualty Care pre-hospital casualty care cards for the US military.[44]

An alternative solution for improving health-related data usage was outlined in a 2011 whitepaper that focused on the existing U.S. Air Force Health Services Data Warehouse (HSDW) that is composed of "federally owned, integrated health systems [that are linked] through an interconnected set of clinical information systems."[45] This warehouse was envisioned to be transformed into "a public resource" for "biomedical and health informatics research" to "improve health services and healthcare" for both military and civilian populations. This whitepaper recommended that "policy and governance frameworks" for this warehouse should include connecting them to "federal and civilian health data repositories."

Cloud Computing: Access and Usage Policies of the Armed Services

In 2015, the Army Chief Information Officer issued the Army Cloud Computing Strategy.[33] For the Army, the concept of cloud computing goes beyond the NIST definition[46] by also considering the conditions in which cloud computing will be operational[33] (see Security Issues below). Another 2015 document from the Department of the Army's CIO noted that the MHS had authority to oversee cloud computing strategies for the U.S. Army Medical Command (MEDCOM) which would continue to follow MHS procedures with the exclusion of its Enterprise applications.[47]

In a counterpoint to the cloud computing policies mentioned above, and stemming from the 2011 whitepaper[45], a 2016 publication described a large-scale clinical informatics platform and database that followed DHA guidelines and was cost-effective.[48] Researchers and organizations were encouraged to use DoD Enterprise-level resources in creating distributed facilities with "their own data repository and trending applications." However, this strategy does not necessarily ensure the affordability that the cloud computing policies seek.

The other armed services have also developed cloud computing policies and documents. The Navy's Cloud First program began reducing its number of on-premises data centers in compliance with a Congressional mandate for the entire DoD.[37] Because the Department of the Navy (DON) anticipated the use of commercial cloud computing services, business case analyses (BCA) would be performed with either the DoD Enterprise IT BCA or the DON Enterprise IT Abbreviated BCA templates.[49] The decision to leverage commercial cloud services was based on an analysis of the costs, security requirements, and the types of stored data.[50]

The Air Force's 2016 cloud contract was the largest in awarded value compared with other defense agencies' cloud contracts.[51] A single hosting system will be provided "for Air Force Information Network core services and functional applications from the Service's major commands, mission offices and program offices." For example, the Air Force's MyPers is an off-premise cloud for sensitive, unclassified data from 1.7 million personnel. In this case, "cost savings are less important than mission performance."[52]

Security Issues

Due to concerns surrounding security and compliance, some organizations have been hesitant to use cloud computing. Security issues requiring the protection of patient data and the security of critical information represent many challenges for cloud implementation due to various regulations, industry standards and legislation.[53] Despite these concerns, a review conducted by the Department of Health and Human Services showed that ~62% (16/25) of large breaches between the years of 2009–2012 involving theft or loss of protected health information (PHI) involved laptops, other portable storage devices, or paper records.[54] At the breach portal of the DHHS, Office of Civil Rights,[21] we searched all seven types of reported breaches (hacking, improper disposal, loss, theft, unauthorized use, unknown and other) through all types of breach locations (i.e., desktops, EHRs, e-mail, laptops, network servers, other portable electronic devices, paper/film, and other) for any covered entity. Breaches that were solely due to network servers that presumably included cloud computers were only 12% (66/550) of the all the recorded breaches. During the extended period from 2009 to 2017, ~16% (260/1638) of all breaches were associated with network servers. These results support the conclusion that the security infrastructure in cloud services are more secure than more traditional IT storage methods in complying with Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulations.[55,56]

The Federal Risk and Authorization Management Program (FedRAMP) was created in 2011 to provide "a comprehensive set of cloud security requirements and an independent assessment program" that was endorsed "by the chief information officers (CIOs) of the DoD, the Department of Homeland

Security (DHS), and the GSA."[35] The lower costs of commercial public cloud platforms were stated to be offset by more expensive security measures required by the DoD.[57] While "the DOD is supposed to use the NIST definition of cloud computing,"[57] the May 2017 Presidential Executive Order 13800[58] states that "each agency head shall use The Framework for Improving Critical Infrastructure Cybersecurity (the Framework) developed by NIST,[59] or any successor document, to manage the agency's cybersecurity risk." That order has been interpreted by different DoD components in various ways. Moreover, according to DISA officials, the NIST definition has not been implemented across the DoD because the Pentagon "is more secure by using customized definitions."[57]

The choice of deployment models (see Methods, Definitions) for the Army cloud-enabled network "is important due to DoD cybersecurity requirements and limitations regarding where DoD data can be hosted."[33] Selection of appropriate deployment models would require evaluations to use the DoD Risk Management Framework (RMF) for DoD IT,[60] the special considerations outlined in NIST 800-144,[61] the various data sensitivity levels (see the DoD Cloud Computing Security Requirements Guide[62]), and the "mission criticality of the system or application."[33]

The costs of implementing a secure cloud infrastructure within the DoD have been examined by the Air University, Air Command, and Staff College.[63] Recommendations from that report included standardizing computer security categorization, implementing a DoD private cloud, and evaluating commercial cloud providers that were the most cost-effective and were associated with the least risk. "Cloud service providers (CSPs) that implement the required security controls and meet independent assessment requirements can be authorized for use by the Federal Government."[64]

Dealing with cybersecurity breaches involves understanding, preventing, and responding to them. Understanding the characteristics of data breaches is a starting point in countering threats to data security. The industry-based 2017 Data Breach Investigations Report[65] has provided detailed statistics in four topic areas. Some specific examples included the perpetrators (75% of breaches conducted by outsiders, 25% by internal actors), their tactics (81% by hacking using weak or stolen passwords, 51% involved malware), their victims (15% involved healthcare organizations), and other common features (66% of malware installed by malicious e-mail attachments).

In 2016, within the realm of healthcare, 458 breach incidents were reported with 296 confirmed data disclosures. Eighty percent of these breaches were due to privilege misuse (e.g., employees accessing data out of curiosity), miscellaneous errors, and physical theft and loss. The compromised information included medical (69%) and personal (33%) data. Ransomware (software that encrypts data and demands payment for their recovery) accounted for 72% of malware incidents, which was approximately one ransomware incident out of every ten total cybersecurity incidents in the healthcare industry in 2016. Some of the data breach prevention methods mentioned included training of users on security awareness, alerting of potential attacks, maintaining security hygiene (keeping security software up to date), and maintaining appropriate credentials. That report also provided recommendations from the Secret Service to help organizations respond quickly and recover from cybersecurity incidents which included the timely enactment of incident response plans and the sharing of threat and incident information.

Assessment of DoD's Usage of Cloud Services

In 2015, the DoD responded to Congressional reports[66,67] by directing the Institute for Defense Analyses (IDA) to conduct an independent assessment of the commercial cloud technologies and services as adopted by the DoD.[68] That IDA study concluded that the DoD offered a substantial number (32) of authorized cloud services "to DoD mission owners" in a variety of configurations having different levels of security. Two of those services offered the hosting of sensitive data (e.g., Personally Identifiable Information, For Official Use Only) with the rest authorized to host non-sensitive, publicly releasable information.

It was determined that the DoD had developed policies and guidance for cloud computing capabilities[62] "that specified key elements that a commercial cloud provider must meet to qualify for each data sensitivity level." IDA reported that "DoD mission owners could also host applications on milCloud," a private cloud that provides infrastructure as a service and leverages enhanced security built by DISA.[69,70] To measure DoD's adoption of cloud technologies, metrics were proposed that included cost reduction, ease-of-use, accessibility, security, and compliance. Finally, the IDA study recommended that DoD consider allowing its Defense Industrial Base partners[71] to use and access "high-sensitivity cloud infrastructures."

CONCLUSIONS

The DoD and other government cloud computing policies developed within the last decade are consistent with the position that sharing health-related research data will foster collaborations among DoD and non-DoD investigators and will increase opportunities to advance military healthcare and reduce potential duplication of effort. This latter topic is especially important in light of Executive Order 13781 "to eliminate unnecessary…agency programs."[72]

The Data Center Consolidation Plan was developed by the OMB in 2011 to avoid low usage and duplicate systems.[1] Cloud technology was intended to reduce the number of data centers, reduce costs, increase energy efficiencies and increase IT security while enhancing support to Service Members.[73] Increased employee mobility, efficiency and productivity were also expected from this technology. Furthermore, even by using only a limited amount of cloud services, the GAO estimated that the government saved one-half billion dollars over approximately four years.[74,75]

In a 2016 GAO report, cloud computing was characterized as being economical, flexible and fast. It was economical because investments were needed only with increased use of the cloud system. It was flexible because the capacity of cloud computing could readily be added or removed, and it was fast in terms of reducing procurement requirements.[74,76–78] From subsequent analyses, the benefits of cloud computing were also considered to include flexibility for scaling up storage capacities, and maintaining resilience, e.g., against automated distributed threats.[58] Overall, consumers of healthcare and health science data would appear to benefit from having access to such computational capabilities that could support collaborative projects, enhance standardization, and be in compliance with federal and DoD data sharing policies and guidances.[79–86]

On the other hand, cloud computing has been associated with transition costs and security issues.[68] Because of this ambiguity, in the 2016 DoD Inspector General (IG) report,[87] it was concluded that the DoD could not measure cloud computing effectiveness or cost savings, in distinct contrast to the 2015 GAO report cited earlier.[74,75] The IG recommended that guidance from the DoD CIO be issued to develop a standard definition for DoD cloud computing or further define the National Institute of Standards and Technology standard. The DoD MHS with its cloud systems could offer some resolution to these problems along with becoming a leader in developing definitions and standards.

Results from our previous survey indicated that limits exist for the 62 unique systems biology-related studies that were being conducted by USAMRMC investigators in 2016.[16] These studies represented a diverse range of experimental designs and approaches, including a variety of large-scale "omics" data. DoD and non-DoD extramural collaborators also played a prominent role in addressing militarily relevant biomedical problems. Most of these systems biology studies were associated with locally stored data that were not readily accessible for sharing. These survey results suggested that USAMRMC researchers and potentially collaborative extramural researchers were hampered by their inability to efficiently share their research data and to generate new solutions to these problem sets. It is our position that their work would be enhanced if investigators had access and used cloud services that could provide a centralized computer facility to store, analyze, search, and share relevant data.

Recommendations

Based on our review of selected government cloud polices, we recommend that cloud computing be considered by DoD biomedical researchers to increase connectivity and, presumably, facilitate communications and data sharing among the various intra- and extramural laboratories. While cloud providers offer trusted services for hosting biomedical research data, any decision to migrate data to a cloud provider needs to be based on an evaluation of the strengths, weaknesses, opportunities, and threats of storing data in an authorized cloud setting. We also recommend that policies and other guidances be updated to include development of additional metrics that will help end-users and other stakeholders evaluate the above mentioned assumptions and expectations.

ACKNOWLEDGEMENTS

Portions of this material were presented at the annual DoD Biotechnologies for Health and Performance: Research, Policy and Operational Applications Workshop, Arlington, VA, July 24–26, 2017.

FUNDING

This work was supported by funds provided by the US Army Medical Research and Materiel Command (USAMRMC).

REFERENCES

1. Kundra V: Federal Cloud Computing Strategy. 2011. Available at https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf, accessed October 12, 2017.
2. Mell P, Grance T: The NIST definition of cloud computing, Special Publication 800-145. 2011. Available at http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf, accessed October 12, 2017.
3. Fang R, Pouyanfar S, Yang Y, Chen S-C, Iyengar S: Computational health informatics in the big data age: a survey. ACM Comput Surv 2016; 49: 1–13.
4. O'Driscoll A, Daugelaite J, Sleator RD: 'Big data', Hadoop and cloud computing in genomics. J Biomed Inform 2013; 46: 774–81.
5. NIH Biennial Report: 2012. Available at https://report.nih.gov/pdf/NIH_Biennial_Report_2012.pdf, accessed October 12, 2017.
6. Human Microbiome Project: 2017. Available at https://portal.hmpdacc.org/search/s?facetTab=cases, accessed October 12, 2017.
7. Einkauf J: Human Microbiome Project – Human Microbiome Project Data Set. 2016. Available at https://aws.amazon.com/datasets/human-microbiome-project/, accessed October 12, 2017.
8. Navas-Molina JA, Hyde ER, Sanders J, Knight R: The microbiome and big data. Curr Opin Syst Biol 2017; 4: 92–96.
9. Broad Institute, Broad moves genome analysis to the cloud; collaborates with cloud providers to offer access to the leading genome analysis toolkit. 2016. Available at https://www.broadinstitute.org/news/8066, accessed October 12, 2017.
10. Zaharia M, Chowdhury M, Franklin MJ, Shenker S, Stoica I: Spark: cluster computing with working sets. HotCloud 2010; 10: 1–7.
11. Mushtaq H, Al-Ars Z: Cluster-based Apache Spark implementation of the GATK DNA analysis pipeline. Bioinformatics and Biomedicine (BIBM), 2015 IEEE International Conference. 2015. IEEE, pp.1471–77
12. Arvidsson S: Automating Model Building in Ligand-based Predictive Drug Discovery Using the Spark Framework. 2015. Uppsala University School of Engineering (Thesis), pp.1–46, Available at https://pdfs.semanticscholar.org/5969/8a99fa0e2f863ed0c90a64672e6160712a8d.pdf, accessed October 12, 2017.
13. Boubela RN, Kalcher K, Huf W, Našel C, Moser E: Big Data approaches for the analysis of large-scale fMRI data using Apache Spark and GPU processing: a demonstration on resting-state fMRI data from the Human Connectome Project. Front Neurosci 2015; 9: 1–8.
14. Taylor RC: An overview of the Hadoop/MapReduce/HBase framework and its current applications in bioinformatics. BMC Bioinformatics 2010; 11 (Suppl 12).

15. Bradburne C, Graham D, Kingston H, Brenner R, Pamuku M, Carruth L: Overview of 'omics technologies for military occupational health surveillance and medicine. Mil Med 2015; 180: 34–48.
16. Zalatoris JJ, Scheerer JB, Lebeda FJ: Collaborative systems biology projects for the military medical community. Mil Med 2017; 182: e1802–09.
17. Chowbina S, Hammamieh R, Kumar R, et al. 2013 SysBioCube: A data warehouse and integrative data analysis platform facilitating systems biology studies of disorders of military relevance. AMIA Jt Summits Transl Sci Proc 2013; 2013: 34–38.
18. Vie LL, Griffith KN, Scheier LM, Lester PB, Seligman ME: The Person-Event Data Environment: leveraging big data for studies of psychological strengths in soldiers. Front Psychol 2013; 4: 1–7.
19. Vie LL, Scheier LM, Lester PB, Ho TE, Labarthe DR, Seligman ME: The US Army Person-Event Data Environment: a military–civilian big data enterprise. Big Data 2015; 3: 67–79.
20. Secretary of the Army, Army Directive 2017-04: Implementation of the Army human capital big data strategy. 2017. Available at http://www.apd.army.mil/epubs/DR_pubs/DR_a/pdf/web/AD2017-04_Final.pdf, accessed October 12, 2017.
21. U.S. Department of Health and Human Services, Office for Civil Rights, Breach Portal: Notice to the Secretary of HHS, Breach of unsecured protected health information 2017. Available at https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf, accessed October 12, 2017.
22. Mell P: What's special about cloud security? IEEE IT Professional 2012; 14: 6–8.
23. Wyld DC: The cloudy future of government IT: cloud computing and the public sector around the world. Int J Web Seman Technol 2010; 2017: 1–20.
24. Kundra V: The White House-Office of Social Innovation and Civic Participation: Streaming at 1:00: In the Cloud. 2009. Available at https://obamawhitehouse.archives.gov/blog/2009/09/15/streaming-100-cloud, accessed October 12, 2017.
25. Kundra V: OMB asks agencies to review data center targets. 2009. Available at https://www.cio.gov/2009/01/01/omb-asks-agencies-to-review-data-center-targets/, accessed October 12, 2017.
26. Figliola PM, Fischer EA: Overview and issues for implementation of the federal cloud computing initiative: Implications for federal information technology reform management. US Congressional Research Service (CRS) 2015. Available at https://pdfs.semanticscholar.org/9704/e204574db1da5e6fcd046a15a43010aa6c23.pdf, accessed October 12, 2017.
27. Kundra V: 25 Point implementation plan to reform federal information technology management. 2010. Available at http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA543512, accessed October 12, 2017.
28. Kundra V: Federal Data Center Consolidation Initiative 2010. Available at https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/assets/egov_docs/federal_data_center_consolidation_initiative_02-26-2010.pdf, accessed October 12, 2017.
29. Kundra V, Spires R: Update on the Federal Data Center Consolidation Initiative. 2010. Available at https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/update-federal-data-center-consolidation-initiative.pdf, accessed October 12, 2017.
30. Scott T: Promoting the use of green IT. 2016. Available at https://obamawhitehouse.archives.gov/blog/2016/08/01/promoting-use-green-it, accessed October 12, 2017.
31. Kundra V: Federal cloud computing strategy presentation. 2011. Available at https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/vivek-kundra-federal-cloud-computing-strategy-02142011.pdf, accessed October 12, 2017.
32. GSA: Federal cloud computing initiative overview. 2010. Available at http://image.lifeservant.com/siteuploadfiles/VSYM/99B5C5E7-8B46-4D14-A53EB8FD1CEEB2BC/FABFD60A-C29A-8FCE-482300C7B6472EF6.pdf, accessed October 12, 2017.
33. Army, CIO/G6: Army Cloud Computing Strategy (v1.1). 2015. Available at http://ciog6.army.mil/Portals/1/Home/Tabs/Strategy/20150424_Army_Cloud_Computing_Strategy.pdf, accessed October 12, 2017.
34. Ribeiro J: NYT: Steven VanRoekel will succeed Kundra as U.S. CIO. 2011. Available at http://www.cio.com/article/2405708/government-use-of-it/nyt–steven-vanroekel-will-succeed-kundra-as-u-s–cio.html, accessed October 12, 2017.
35. VanRoekel S: Security authorization of information systems in cloud computing environments. 2011. Available at https://www.fismacenter.com/fedrampmemo.pdf, accessed October 12, 2017.
36. DoD, Chief Information Officer, Report: Cloud Computing Strategy. 2012. Available at http://www.dtic.mil/get-tr-doc/pdf?AD=ADA563989, accessed October 12, 2017.
37. National Defense Authorization Act for Fiscal Year 2012, Public Law 112–81—DEC. 31, 2011 2012. Available at https://www.treasury.gov/resource-center/sanctions/Programs/Documents/ndaa_publaw.pdf, accessed October 12, 2017.
38. DoD, Chief Information Officer, Report: DoD Information Technology (IT) Enterprise Strategy and Roadmap, Version 1.0 – 6 SEP 11. 2011. Available at https://pdfs.semanticscholar.org/5ae6/6a9a3cbc3c2c6a044c5b5c728357f5bafe28.pdf?_ga=2.237675712.1103955481.1501266886-577701389.1501266886, accessed October 12, 2017.
39. DoD, Chief Information Officer, Memorandum: Updated guidance on the acquisition and use of commercial cloud computing services. 2014. Available at http://dodcio.defense.gov/Portals/0/Documents/Cloud/DoD%20CIO%20-%20Updated%20Guidance%20-%20Acquisition%20and%20Use%20of%20Commercial%20Cloud%20Serviices_20141215.pdf, accessed October 12, 2017.
40. Assistant Secretary of Defense, Health Affairs, Memorandum: Military Health System Cloud First adoption directive and policy guidance. 2012. Available at http://www.health.mil/Policies/2012/05/22/MHS-Cloud-First-Adoption-Directive-and-Policy-Guidance-Signed-Memo-and-Attachment, accessed October 12, 2017.
41. Defense Health Agency, Director, Memorandum: Defense Health Agency use of cloud computing and hosting services. 2016. Available at https://sysbiocube-abcc.ncifcrf.gov/public/sysbiocube_documents/sysbiocube_data_policy/2016-DHA-Cloud-Policy.pdf, accessed October 12, 2017.
42. Hsiao C-J, King J, Hing E, Simon AE: The role of health information technology in care coordination in the United States. Med Care 2015; 53: 184–90.
43. Defense Health Agency: Health Information Technology (HIT) Research Directory 2016. Available at https://health.mil/Military-Health-Topics/Technology/Support-Areas/Health-IT-Research-and-Innovation, accessed October 12, 2017.
44. Poropatich R, Presson N, Gilbert G: Telemedicine and mHealth odyssey: A journey from the battlefield to academia. SPIE Defense + Security 2016, pps. 1-8. Available at https://www.spiedigitallibrary.org/conference-proceedings-of-spie/9836/98360V/Telemedicine-and-mHealth-odyssey–a-journey-from-the-battlefield/10.1117/12.2223333.short?fileName=98360V, accessed October 12, 2017.
45. Agarwal R, Carnahan D, Crowley P, Bonnema A, Calvo A, Eisen S, Sanderson IC: Leveraging the Air Force Health Services Data Warehouse for transformational healthcare research: An action agenda for the health informatics research initiative. AMIA (Whitepaper) 2011. Available at http://www.rhsmith.umd.edu/files/Documents/Centers/CHIDS/LeveragingHSDW.pdf, accessed October 12, 2017.
46. NIST: Information Technology Laboratory: Big Data Information. 2016. Available at https://www.nist.gov/el/cyber-physical-systems/big-data-pwg, accessed October 12, 2017.
47. Army, Chief Information Officer/G-6, Memorandum: guidance for migration to, and use of, commercial Cloud Service Providers (CSPs). 2015. Available at http://ciog6.army.mil/Portals/1/PolicyLegislation/ArmyITPolicyDocuments/2015/CloudStrategy07312015.pdf, accessed October 12, 2017.

48. Caban JJ, Bonnema A, Bueno ER, DeGraba T, Grammer G, Greenhalgh W, Kass S: A large-scale informatics database to advance research and discovery of the effects of mild traumatic brain injury. Mil Med 2016; 181: 11–22.
49. Department of the Navy, Chief Information Officer, Memorandum: Acquisition and use of commercial cloud computing services. 2015. Available at http://www.doncio.navy.mil/ContentView.aspx?ID=6406, accessed October 12, 2017.
50. Cohen R: U.S. Navy issues new cloud computing policy. 2013. Available at https://www.forbes.com/sites/reuvencohen/2013/04/08/u-s-navy-issues-new-cloud-computing-policy/#3395004f7db4, accessed October 12, 2017.
51. Rockwell M: Air Force has biggest cloud contract in 2016. Available at https://fcw.com/Articles/2016/10/07/Cloud-contracts-2016.aspx?p=1, accessed October 12, 2017.
52. Konkel F: One of Air Force's most important unclassified systems is now in the Oracle cloud. 2016. Available at http://www.nextgov.com/cloud-computing/2016/10/one-air-forces-most-important-unclassified-systems-now-oracle-cloud/132298/, accessed October 12, 2017.
53. DoD Cloud Connection Process Guide, V. 2. 2017. Available at http://www.disa.mil/~/media/Files/DISA/Services/DISN-Connect/References/CCPG.pdf, accessed October 12, 2017.
54. Holtzman D: Breach notification for HIPAA covered entities and business associates. 2012. Available at http://csrc.nist.gov/news_events/hiipaa_june2012/day2/day2-4_dholtzman_ocr-hitech-breach-notifcation-rule.pdf, accessed October 12, 2017.
55. Public Law 104-191 Health Insurance Portability and Accountability Act of 1996. 1996. Available at https://www.nationallibertyalliance.org/sites/default/files/HIPA.pdf, accessed October 12, 2017.
56. Fogarty D: The healthcare cloud and Defense Health Agency: the what, why, and when. 2015. Available at http://www.seguetech.com/healthcare-cloud-defense-health-agency/, accessed October 12, 2017.
57. Goldstein P: Air Force CTO puts focus on cloud governance and cost. 2015. Available at https://fedtechmagazine.com/article/2016/01/air-force-cto-puts-focus-cloud-governance-and-cost, accessed October 12, 2017.
58. Executive Order 13800: Strengthening the cybersecurity of federal networks and critical infrastructure. 2017. Available at https://www.gpo.gov/fdsys/pkg/FR-2017-05-16/pdf/2017-10004.pdf, accessed October 12, 2017.
59. NIST: Framework for improving critical infrastructure cybersecurity. 2014. Available at https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf, accessed October 12, 2017.
60. DoD, Chief Information Officer, DoD Instruction: Risk Management Framework (RMF) for DoD information technology (IT). 2014 (incorporating Change 2, effective July 28, 2017). Available at http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001_2014.pdf, accessed October 12, 2017.
61. Jansen W, Grance T: SP 800-144. Guidelines on security and privacy in public cloud computing. 2011. Available at http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf, accessed October 12, 2017.
62. DoD, Defense Information Systems Agency, Report: Cloud Computing Security Requirements Guide, Version 1, Release 3. 2017. Available at https://iasecontent.disa.mil/cloud/Downloads/Cloud_Computing_SRG_v1r3.pdf, accessed October 12, 2017.
63. Dudash SC: The Department of Defense and the Power of Cloud Computing: weighing acceptable cost versus acceptable risk. 2016. Available at http://www.dtic.mil/get-tr-doc/pdf?AD=AD1015712, accessed October 12, 2017.
64. Taylor L: FedRAMP: History and future direction. IEEE Cloud Comput 2014; 1: 10–4.
65. Verizon Enterprise Solutions, Data Breach Investigations Report, 10th edition, pp. 1–76. 2017. Available at http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/, accessed October 12, 2017.
66. U.S. House of Representatives Report 113-446 National Defense Authorization Act for Fiscal Year 2015. 2014. Available at https://www.congress.gov/113/crpt/hrpt446/CRPT-113hrpt446.pdf, accessed October 12, 2017.
67. U.S. Senate Report 113-176 National Defense Authorization Act for Fiscal Year 2015. 2014. Available at https://www.congress.gov/113/crpt/srpt176/CRPT-113srpt176.pdf, accessed October 12, 2017.
68. Odell LA, Wagner RR, Weir TJ: Department of Defense use of commercial cloud computing capabilities and services (IDA Paper P-5287). 2015. Available at http://www.dtic.mil/dtic/tr/fulltext/u2/1002758.pdf, accessed October 12, 2017.
69. Sanders CG: Insights from exploration into cloud-based simulation. 2014. Available at https://www.researchgate.net/profile/Charles_Sanders3/publication/281827674_Insights_from_Exploration_into_Cloud-based_Simulation/links/55f9d5e308aeafc8ac29c5f0.pdf, accessed October 12, 2017.
70. DISA: milCloud. 2017. Available at http://www.disa.mil/Computing/Cloud-Services/MilCloud, accessed October 12, 2017.
71. Michett V: DoD's Defense Industrial Base Cybersecurity (DIB CS) Program. 2016. Available at https://www.fbcinc.com/e/cybertexas/presentations/Room_302_Wed_1-145PM_Vicki_Michetti_DIB_101_Cyber_Texas_Aug15.pdf, accessed October 12, 2017.
72. Executive Order 13781: Comprehensive plan for reorganizing the executive branch. 2017. Available at https://www.hsdl.org/?view&did=799505, accessed October 12, 2017.
73. Ku M: Department of the Navy push to the cloud: PEO EIS leading the way for commercial cloud acquisition. 2017. Available at http://www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=8939, accessed October 12, 2017.
74. GAO: Information Technology Reform – Billions of dollars in savings have been realized, but agencies need to complete reinvestment plans. 2015. Available at http://www.gao.gov/assets/680/672916.pdf, accessed October 12, 2017.
75. Breeden J: A tool that can keep federal data centers safe amid cloud chaos. 2017. Available at http://www.nextgov.com/technology-news/tech-insider/2017/07/tool-can-keep-federal-data-centers-safe-amid-cloud-chaos/139700/?oref=ng-relatedstories, accessed October 12, 2017.
76. GAO, Report: Cloud Computing – agencies need to incorporate key practices to ensure effective performance. 2016. Available at http://www.gao.gov/assets/680/676395.pdf, accessed October 12, 2017.
77. Lewin K: Federal cloud computing initiative overview. 2009. Available at http://image.lifeservant.com/siteuploadfiles/VSYM/99B5C5E7-8B46-4D14-A53EB8FD1CEEB2BC/FABFD60A-C29A-8FCE-482300C7B6472EF6.pdf, accessed October 12, 2017.
78. GSA, Report: Best business practices for USG cloud adoption. 2016. Available at https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwjDoP6h1-3WAhXCPiYKHUHmAsEQFgg6MAA&url=https%3A%2F%2Fapp_gsagov_prod_rdcgwaajp7wr.s3.amazonaws.com%2FGSACloudBestBusinessPractices.pdf&usg=AOvVaw2UNzgD2KW20veNK1E_sZl9, accessed October 12, 2017.
79. Office of Science and Technology Policy, Memorandum: Increasing access to the results of federally funded research. 2013. Available at https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/ostp_public_access_memo_2013.pdf, accessed October 12, 2017.
80. Office of Management and Budget, Memorandum M-13-13: Open data policy-managing information as an asset. 2013. Available at https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2013/m-13-13.pdf, accessed October 12, 2017.
81. Executive Order 13642: Making open and machine readable the new default for government information. Federal Register, 2013; 78: 28111–28113.
82. Office of Management and Budget, Report: Comprehensive data inventory. 2016. Available at https://obamawhitehouse.archives.gov/sites/default/files/omb/mgmt-gpra/comprehensive_data_inventory.pdf, accessed October 12, 2017.
83. Under Secretary of Defense for Acquisition, Technology and Logistics, Memorandum: Public access to the results of Department of Defense-

funded research. 2014. Available at http://dtic.mil/dtic/pdf/PublicAccessMemo2014.pdf, accessed October 12, 2017.
84. Department of Defense: Plan to establish public access to the results of federally funded research. 2015. Available at http://www.dtic.mil/dtic/pdf/dod_public_access_plan_feb2015.pdf, accessed October 12, 2017.
85. Interagency Working Group on Open Data Sharing Policy of the Subcommittee on International Issues of the Committee on Science of the National Science and Technology Council: Principles for promoting access to Federal Government-supported scientific data and research findings through international scientific cooperation. 2016. Available at http://www.nesdisia.noaa.gov/docs/iwgodsp_principles_0.pdf, accessed October 12, 2017.
86. Under Secretary of Defense for Acquisition, Technology, and Logistics, Directive-type Memorandum (DTM) 17-002: Public access to the results of DoD intramural basic research published in peer reviewed scholarly publications. 2017. Available at http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dtm/DTM-17-002.pdf, accessed October 12, 2017.
87. DoD Inspector General: DoD needs an effective process to identify cloud computing service contracts. 2016. Available at http://www.dodig.mil/pubs/documents/DODIG-2016-038.pdf, accessed September 13, 2017.
88. National Defense Authorization Act for Fiscal Year 2015.1 [Pub. L. No. 113-291, division A, title VIII, subtitle D, 128 Stat. 3292, 3438]. December 19, 2014. Available at https://www.congress.gov/113/plaws/publ291/PLAW-113publ291.pdf, accessed October 12, 2017.
89. Secretary of the Army, Army Directive 2016-38: Migration of army systems and applications to approved hosting environments and consolidation of data centers. 2016. Available at http://www.apd.army.mil/epubs/DR_pubs/DR_a/pdf/web/AD2016-38_Final.pdf, accessed October 12, 2017.
90. Office of Management and Budget, Memorandum: M-16-19: The Data Center Optimization Initiative (DCOI). 2016. Available at https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2016/m_16_19_1.pdf, accessed October 12, 2017.