Staying Safer in Cyberspace: Cloud Security on the Horizon

January 2014

Karen S. Evans
Julie M. Anderson
Brian D. Shevenaugh

SafeGov
Executive Summary

Since announcing its “Cloud First” policy in 2010, the Federal government has correctly identified cloud computing as a way to reduce costs and improve the use of existing assets, and has accordingly prioritized its adoption. It has also taken judicious steps to protect Federal networks from nefarious cyber-attacks and promote the dissemination of best practices for cybersecurity. The Federal government has also embraced mobility as a means to conduct work from any location. But until now, the implementation of these initiatives has been fragmented and lacked coordination across Federal agencies.

This paper offers a framework for integrating these programs in a way that enables the Federal government to realize the economic, technological, and mission-effectiveness benefits of cloud services while simultaneously meeting current Federal cybersecurity requirements. It advocates shifting from a compliance-based cybersecurity paradigm to one that is risk-based and focusing on how to most effectively secure their implementation of cloud services.

Recommendations

The following recommendations will help Federal entities better integrate the various Federal programs relating to cloud computing and cybersecurity:

1. Within the next year, the Information Security Identity Management Committee (ISIMC) of the Federal Chief Information Officer (CIO) Council should adopt and issue an integrated network architecture to address the Administration’s priorities and help agencies implement Federal cybersecurity requirements, including the Cross Agency Performance (CAP) Cybersecurity Goals; Open Government; the Data Center Consolidation Initiative; Cloud Services; and Mobility.

---

1 See the “25 Point Implementation Plan to Reform Federal Information Technology Management” (Vivek Kundra, 2010).
A. Additionally, the ISIMC should draft a notional implementation plan with the milestones outlined to help the agencies transition from their current architectures to the proposed architecture that includes these enhancements.

B. This should be coordinated with the Inspectors General (IGs) to ensure that the evaluations conducted under Federal Information Security Management Act (FISMA) use the recommended architecture, standards, and transition plans—instead of selecting their own monitoring plans based on National Institute of Standards and Technology (NIST) publications that do not consider agency implementation plans.

2. FedRAMP’s Joint Authorization Board (JAB) should require that all cloud service providers wishing to do business with the Federal government employ penetration testing capabilities in the implemented operational environment in order to surveil, analyze, and respond to threats in real-time. This process of testing whether computing systems have been penetrated could be similar to the Payment Card Industry’s Data Security Standard (PCI DSS), which is a well-established set of industry benchmarks for online payment services.

Industry and government must decide together what will be subjected to penetration testing. Adopting the model contracting language included in Appendix 3 would help these entities arrive at a consensus on these and other issues while requiring:

A. All commercial cloud services be integrated with Federal security protections such as the Trusted Internet Connection (TIC) and Homeland Security Presidential Directive (HSPD) 12 for identity management.

B. Cloud service providers share log files with the contracting Federal agencies and/or directly with the Department of Homeland Security’s (DHS) Continuous Diagnostics and Mitigation (CDM) program.³

C. The Federal government, in conjunction with Cloud Service Providers, resolves the multi-tenancy⁴ issues associated with the sharing of these data.

³ [http://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-03.pdf](http://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-03.pdf)

⁴ When multiple clients inhabit a single cloud.
3. Office of Management and Budget (OMB) and Department of Homeland Security (DHS) should **work together to develop and issue metrics that inspectors general (IGs) can use to assess the effectiveness of cybersecurity measures in the FISMA reporting process.**

   A. We proposed a Cyber Risk Indicator in our 2013 paper, “Measuring What Matters,” which argues that cybersecurity risk depends on the performance of an agency’s information systems and the maturity of attendant information security policies and processes. We also contend that these factors need to be assessed in the context of organizational priorities.

   B. The ISIMC should continue to further define the benefits and metrics associated with the DHS’ CDM program.

4. OMB and the National Security Staff (NSS) should:

   A. Ensure that cybersecurity planning and architecture efforts of the ISIMC and the Committee for National Security Systems are aligned whenever possible; and

   B. Hold departments and agencies accountable by assessing their progress towards fulfilling agreed-upon cybersecurity requirements.

**Conclusion**

At a time when the Federal government is facing ever-mounting budgetary pressures, cloud computing can be a useful tool to help agency leaders to deliver mission services while managing expenditures. And in a recent poll, nearly half of all senior national security officials also named cyberwarfare as “the most serious threat facing the United States.” The “Staying Safer in Cyberspace” plan we present in this paper differs from the current fragmented approach to securing the cloud by identifying an integrated approach and a coordinating body to develop a network architecture that conforms to

---

5 In its September 2013 report, the GAO recommended that DHS and OMB work together to create effectiveness metrics to be used in the FISMA reporting process (GAO, *Federal Information Security: Mixed Progress in Implementing Program Components; Improved Metrics Needed to Measure Effectiveness,* September 2013, p. 45).

6 http://www.defensenews.com/article/20140105/DEFREG02/301050011
the Administration’s cybersecurity policies. What’s more, it describes the contours of what this network architecture should look like—from performance metrics down to identity management practices at the end user level. These recommendations delineate essential functions for both the private sector and the Federal government, while allowing for discussion about certain details. Similarly, our plan also allows room for the unique security requirements of departments and agencies to be considered, all within the framework of existing legislation.
Table of Contents

1: Introduction ........................................................................................................................................... 7
   The Promise of the Cloud ....................................................................................................................... 8
   Securing the Cloud and Federal Networks .......................................................................................... 9
   Challenges to Implementing the Existing Federal Network Security Framework as It Applies to the Cloud ............................................................................................................................ 12

2: Plan to Secure Cloud Implementation for Federal Agencies .......................................................... 16
   Recommendation 1: ISIMC Should Adopt and Issue an Integrated Network Architecture ............... 16
   Recommendation 2: FedRAMP’s JAB Should Require Penetration Testing among Cloud Service Providers .......................................................................................................................... 18
   Recommendation 3: Use HSPD-12 Credentials to Validate Identity for Federal Employees .............. 19
   Recommendation 4: Cloud Service Providers Must Share Aggregate System Log Files with Federal Agencies under Continuous Diagnostics and Mitigation ................................................. 19
   Recommendation 5: OMB and DHS Should Develop and Issue Effectiveness Metrics for IGs to Use in FISMA Reporting ........................................................................................................... 20
   Desired Outcomes .................................................................................................................................... 21

3: Challenges in Implementing the Plan .................................................................................................. 22
   Conclusion ................................................................................................................................................. 23

Appendix 1: Defining the Cloud ................................................................................................................. 24
Appendix 2: Overview of “Cloud First” ..................................................................................................... 25
Appendix 3: Model Language for Federal Cloud Contracts .................................................................... 27
Glossary ....................................................................................................................................................... 31
About the Authors ....................................................................................................................................... 32
1: Introduction

Cloud computing brings with it both risks and rewards. In recent years, senior Federal officials from the Secretary of Defense to the Director of National Intelligence and even the President have stressed that securing our information systems and computer networks is a crucial element of the nation’s security architecture.\textsuperscript{7} At the same time, the Federal government is turning to cloud computing to resolve some of the problems that have chronically plagued its information technology (IT) environment.\textsuperscript{8} But until now, efforts to implement cybersecurity and cloud computing initiatives have been too fragmented and lacked the type of overarching coordination needed to mitigate the risks while reaping the rewards. This paper offers a plan to help agency CIOs realize the benefits of cloud technology while meeting current Federal cybersecurity requirements.

This paper was developed through a collaborative process with experts from both the private and public sectors. The project team first held consultative conversations with senior leaders from Federal CIO Council, Department of Defense, Department of Homeland Security, Department of Justice, and members of SafeGov.org. The team attempted to adjudicate the resulting ideas and incorporated them into the plan as appropriate. Rough drafts of this paper were shared with key stakeholders across the public and private sectors. It is important to note that the plan addresses only unclassified data and networks.

In this section of the paper, we first outline the benefits of cloud computing in general and what it can do for the Federal government. In the second part, we describe Federal efforts to secure cloud services. In the third part, we outline the challenges to implementing the current policies. Finally, we cover our proposed solution.\textsuperscript{9}

\textsuperscript{7} GAO, September 2013, p. 2.  
\textsuperscript{8} Kundra, Vivek. Federal Cloud Computing Strategy. (February 2011, pg. 1). The current Administration’s Data Center Consolidation Initiative is attempting to address these issues, although it has been met with problems of its own.  
\textsuperscript{9} Appendixes 1 and 2 define the term “cloud computing” and outline the Federal government’s cloud computing initiatives, respectively.
The Promise of the Cloud

Cloud computing is a powerful tool that can help meet some of the most pressing information management, cybersecurity, and transparency challenges facing the Federal IT environment. In the 2011 Federal Cloud Computing Strategy (FCCS), then-U.S. CIO Vivek Kundra characterized the government’s IT systems as plagued by low asset utilization, fragmented resource demand, and duplicative IT systems. He cited an August 2010 Office of Management and Budget (OMB) survey, which determined that many agencies were using less than 30% of their available server capacity. Recently, it has become clear that the sheer number of Federal data centers further fragments and duplicates IT assets. A July 2013 Government Accountability (GAO) report found that the number of Federal data centers now likely exceeds 7,000—twice the number originally intended.

Cloud computing’s demand aggregation properties can help mitigate some of these pathologies by concentrating security expertise and capabilities, which could be leveraged across the cloud environment. Agencies use Federal IT assets infrequently, in part because they must retain some reserve capacity to accommodate cyclical or unanticipated spikes in demand. With their elasticity and metering functions, cloud services enable clients to access more resources during times of peak demand, thereby enabling agencies to best use their assets. As the FCCS points out, sharing and pooling IT resources through cloud services can also “complement data center consolidation efforts by shifting workloads and applications to infrastructures owned by third parties.”

By adopting cloud services, the Federal government could save substantially. Kundra has estimated that $20 billion of the Federal government’s $80 billion annual IT budget could potentially be migrated to the cloud. He singled out data center expenditure as being particularly ripe for cloud savings, projecting a nearly 30% reduction in this

---

12 This dramatic increase is in part due to re-defining the square footage criteria for categorizing facilities as data centers. http://www.informationweek.com/government/policy/lawmakers-grill-federal-cio-on-data-cent/240158975
category. Forbes cited MeriTalk Cloud Computing Exchange as predicting that the shift from “on-premise systems to cloud-based systems” could save the government more than $12 billion, or 7% of its annual IT budget. OMB has estimated the savings at $5 billion per year, although Kundra emphasized that this is the lowest possible figure.

Securing the Cloud and Federal Networks

While cloud computing offers numerous potential advantages, it also presents security risks that must be carefully managed. This section explores both the general security issues associated with cloud computing and two foundational elements of the Federal government’s effort to safeguard its networks: the CAP Goal on Cybersecurity and the Federal Information Security Management Act (FISMA).

General Cloud Security Considerations

Although cloud computing presents unique security challenges, which must be carefully managed, it offers several benefits over other forms of network design. By centralizing otherwise atomized computing services, cloud networks provide attackers with a larger target, amplifying the payoff of a successful intrusion. For certain categories of cloud services, this sharing of computing resources among multiple customers may create a “multi-tenancy” problem when end users have different security requirements. However, by concentrating services, cloud computing makes it easier to build the type of standardized, layered security protocols required to protect against cyber-attacks. What’s more, the economies of scale achieved by pooling resources allow the cloud provider to invest more effectively in security software, infrastructure, and personnel. Cloud networks certainly require robust identity credentials, but the benefits accrued in other areas make the investment worthwhile.

---

19 These are general Federal cybersecurity measures. We will outline how they apply to cloud computing, and why they must be changed, in the next section.
20 The “multi-tenancy” problem may not be as acute in more highly abstract cloud computing environments, such as Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). See Fischer, Eric. “Overview and Issues for Implementation of the Federal Cloud Computing Initiative: Implications for Federal Information Technology Reform Management.” Congressional Research Service. (2013, p. 11).
Cross Agency Priority Cybersecurity Goal

The current administration has identified cybersecurity as one of its fifteen CAP Goals.\textsuperscript{21} The CAP Cybersecurity Goal focuses on achieving three priority capabilities: continuous monitoring, Trusted Internet Connections (TIC), and strong authentication. The weighted average of U.S. government-wide adoption of these capabilities declined from 81.28\% in Q2 to 80.14\% in FY2013—which falls short of the CAP target set for that year.\textsuperscript{22} These capabilities are summarized and explored in greater detail below:

Security of Federal Information and Information Systems: “Transform the historically static security control assessment and authorization process into an integral part of a dynamic enterprise-wide risk management process. This change allows departments and agencies to maintain an ongoing near-real-time awareness and assessment of information security risk and rapidly respond to support organizational risk management decisions.”\textsuperscript{23}

NIST defines continuous security monitoring as “a risk management approach to cybersecurity that maintains a picture of an organization’s security posture, provides visibility into assets, leverages use of automated data feeds, monitors effectiveness of security controls, and enables prioritization of remedies.”\textsuperscript{24} The CDM program falls within DHS’s broad information security mandate. In 2010, OMB designated DHS as having the responsibility to “oversee and assist government-wide and agency-specific efforts to provide adequate, risk-based and cost-effective cybersecurity.”\textsuperscript{25} Underscoring the importance of continuous diagnostics and mitigation policing, DHS pointed out that 80\% of exploits take advantage of known vulnerabilities and weaknesses in configuration management settings. It also notes that the Federal government experienced 106,000 cyber-attacks in 2011—or roughly 290 per day.\textsuperscript{26} Departments and agencies must reduce the time required to detect, localize, and mitigate malicious code on government networks and assets when implemented in the cloud.

\textsuperscript{21} CAP Goals are part of the current administration’s Accountable Government Initiative, which aims to evaluate agency progress toward these milestones using a “data-driven” approach (http://www.whitehouse.gov/the-press-office/2010/09/14/presidential-memorandum-accountable-government-initiative). Information on the fourteen other CAP Goals can be found here: http://goals.performance.gov/goals_2013.
\textsuperscript{23} FY2013 Q2, “CAP Cyber Progress Update.” p. 6.
\textsuperscript{25} DHS. “Implementing Continuous Monitoring To Better Protect Federal Networks and Data.” (2012, p. 1).
\textsuperscript{26} DHS. “Implementing Continuous Monitoring To Better Protect Federal Networks and Data.” (2012, p. 1).
Trusted Internet Connections (TIC): “Consolidate external Internet traffic and ensure a set of common security capabilities for situational awareness and enhanced monitoring.”

Originally outlined in OMB Memorandum M-08-05 (2007), the TIC initiative aims to “optimize [the Federal government’s] individual network services into a common solution” by reducing and consolidating the number of external access points to a target of 50. Agencies can connect to external access points either via other agencies that OMB has designated as TIC Access Providers (TICAP), or via commercial carriers that have been selected as Managed Trusted IP Service (MTIPS) providers. The Networx contract is the only vehicle through which Federal civilian agencies in the U.S. may procure TIC-compliant services. TICAPs are allowed a maximum of two TICs, which means that through a combination of TICAPs and MTIPS, agencies can use 8-10 TIC access points.

As currently stated, the policy is narrowly defined and focused on a “perimeter-style” defense. This policy requirement must be integrated into the push for cloud, mobility, and identity management initiatives in order to create a workable Federal operating environment.

Strong Authentication: “Ensure only authorized employees have access to Federal information systems by requiring a higher level of assurance following the HSPD-12 Personal Identity Verification standard.”

Issued in 2004, the Homeland Security Presidential Directive 12 (HSPD-12), titled, “Policy for a Common Identification Standard for Federal Employees and Contractors,” established a “mandatory, Government-wide standard for secure and reliable forms of identification” in an effort to enhance security, reduce identity theft, and protect personal privacy. OMB was responsible for overseeing agency implementation of this initiative. To this end, the technology has advanced to two-factor authentication for

---

29 It should be noted that these still are not designed for multitenant, cloud service provider, or “mesh” networking. http://www.dhs.gov/trusted-internet-connections
31 Ibid., p. 7
32 FY2013 Q2, CAP Cyber Progress Update, p. 7.
33 http://www.dhs.gov/homeland-security-presidential-directive-12
34 http://www.whitehouse.gov/omb/e-gov/hspd12_reports
network access, in which the user’s identity is verified with multiple credentials.\(^{35}\) HSPD-12 must be aligned with the current administration’s initiative, “National Strategy for Identities in Cyberspace”\(^ {36}\) and provide recommendations for cloud service providers in order achieve the identity requirements and expectations contained in the initiative.

**FISMA**

Enacted in 2002, FISMA seeks to create a “comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets.” It provides for “minimum controls” to protect Federal networks, while acknowledging that the “selection of specific technical hardware and software information security solutions should be left to individual agencies.”\(^ {37}\) FISMA requires agency heads to provide security protections that are proportionate to their level of risk and the magnitude of a security breach,\(^ {38}\) while emphasizing that these solutions must be cost-effective.\(^ {39}\) It also requires the head of each agency to take an inventory of the agency’s major information systems.\(^ {40}\)

**Challenges to Implementing the Existing Federal Network Security Framework as It Applies to the Cloud**

In order for the agencies to adopt a risk-based approach to securing their overall IT portfolio while revamping it to incorporate cloud computing, they must be able to fully integrate existing cybersecurity initiatives. Although agency CIOs have always faced the challenge of implementing their agency-specific needs in conjunction with government-wide initiatives, current Federal cybersecurity efforts have been particularly difficult to integrate. For one thing, the FISMA reporting process emphasizes compliance over effectiveness. Similarly, agencies have been uneven in implementing testing and evaluation programs. Furthermore, the TIC network topology defines cloud services as

---

\(^{35}\) Two-factor authentication is often described as requiring “something you have,” such as a Personal Identity Verification (PIV) card, and “something you know,” such as a password, in order to gain access to a network or service. For example, this is different than the security standards typically used when accessing personal email accounts, which typically require only a password. Two-factor authentication incorporates a physical component into the identity verification process.


\(^{37}\) HR 2458, FISMA, Section 3541 (1), p. 48.

\(^{38}\) Ibid., p. 49-50.

\(^{39}\) Ibid., p. 51.

\(^{40}\) Ibid., p. 63.
external connections without requiring the use of identity management and authorization to access application and data services. Finally, recent budget constraints have often compelled agency CIOs to prioritize the cost of their IT solutions and cloud services over security and functionality during the procurement process. Below we explore how these issues are impeding Federal initiatives in cybersecurity and cloud computing.

**FISMA Compliance Emphasized Over Effectiveness**

Although FISMA directs agencies to manage their risk, in practice FISMA assessors too often employ a “check-the-box” approach to information security. A September 2013 Government Accountability Office (GAO) report on Federal information security found that in the process of issuing their mandatory FISMA updates to DHS, IGs too often focus simply on reporting their compliance with this law rather than on assessing the effectiveness of their cybersecurity programs:

> For each control category, the metrics ask whether the agency established an enterprise-wide program that was consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. However, these metrics do not allow the inspectors general to respond on how effectively the program is operating. Instead, they capture whether programs have been established.41

Keith Rhodes, former chief technologist and director of the GAO’s Center for Technology and Engineering, has warned of the dangers of allowing FISMA to become a mere “paper exercise.”42 Greater emphasis should be placed on determining whether agency cybersecurity programs demonstrably improve the security of Federal IT assets and whether they fully address the risks agencies face. Elsewhere, we have argued that FISMA-based security measures must shift their focus from mere compliance to a more risk-based approach to cybersecurity.43

**Uneven Implementation of Test and Evaluation Programs**

The same GAO report states that 17 of 24 agency IGs found weaknesses in agency processes for testing and evaluating security controls. In particular, 10 of 23 agencies “did not monitor information security controls on an ongoing basis” in FY2012. Without

---

41 GAO, September 2013, p. 38.
these programs in place, agencies will not be fully aware of vulnerabilities in their critical information systems. This absence of testing and evaluation capabilities further demonstrates the lack of emphasis on evaluating security effectiveness among many agencies. In addition, agencies are inconsistent in their testing and evaluation activities. IGs test and evaluate controls as outlined in NIST publications, but risks would be more effectively identified and managed by standardized evaluation procedures that create a baseline for measurement and improvement.

**TIC Does Not Require Strong Authentication When Accessing Cloud Services**

The goal of the TIC initiative is to enhance Federal cybersecurity by limiting the number of connections—thus reducing the vulnerability of agency information systems. Under its current iteration, TIC defines cloud providers as external connections because the department or agency (D/A) procuring cloud services “does not have control over the application of required security controls or the assessment of security control effectiveness on the outside information system, network, or components of information systems or networks.” Even though this definition acknowledges that D/As do not administer the security protocols at the other end of the connection, the current TIC architecture does not require Federal employees to use a robust system of authentication when accessing services, applications, or data implemented in the external cloud solution (as the table on the next page illustrates). This applies to both Federally-controlled and commercially-managed cloud solutions.

The absence of strong authentication systems when connecting to cloud services through a TIC presents a major security vulnerability. Access to cloud services is currently protected by PIN and password security solutions, but these defenses are only as strong as the user’s passcode. There are several examples of agencies experiencing cyber-attacks, with the most recent being a breach at the Department of Energy in July 2013 in which the personally identifiable information (PII) of almost 53,000 current and former departmental employees was compromised. If hackers have sufficient PII on Federal employees, they can then contact the agency’s IT services posing as that person and request a password reset in order to gain access to more sensitive networks. Incidents such as these demonstrate the need for a more robust form of authentication than is currently in place under the TIC initiative.

---

44 GAO, September 2013, p. 19.
In Agency CIO’s Calculus, Cost often Trumps Security and Functionality

When procuring cloud services, agency CIOs generally take into account three main factors: the cost of the services, the level of security the provider offers, and the functionality of these services. This is consistent with a “total cost of ownership” approach to IT asset acquisition that is mandated by OMB. However, because of the current austere budgetary environment, agency CIOs are often compelled to choose the cheapest technically-acceptable services that are available. Rarely, however, do agency CIOs take into account the cost of an actual security breach, which can leak sensitive national security or economic information. There can be further recovery and credit monitoring costs if personally-identifiable information is lost in the breach. Under these circumstances, paying a little more for a higher level of cloud security can prove more cost-effective.

Figure 1. “Notional TIC Architecture.”

http://www.whitehouse.gov/omb/memoranda_fy04_m04-16/

OMB identifies credit monitoring as a useful but “costly” measure to counteract the effects of a security breach involving government-issued credit cards. http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2006/task_force_theft_memo.pdf
2: Plan to Secure Cloud Implementation for Federal Agencies

Agency CIOs must be able to integrate all of their information security initiatives in order to effectively implement and maintain mission-based IT solutions. This report recommends the measures listed below to improve the current Federal security architecture while pursuing the “Cloud First” imperative. Appendix 2 describes the Cloud First policy.

Recommendation 1: ISIMC Should Adopt and Issue an Integrated Network Architecture

The Information Security Identity Management Committee (ISIMC) of the Federal CIO Council should adopt an integrated architecture addressing the Administration’s priorities to assist agencies in implementing the CAP Cybersecurity Goals; Open Government; the Data Center Consolidation Initiative; Cloud Services; and Mobility.

This architecture should be similar to the enhancement made to the existing TIC architecture which includes the Federal bridge as outlined in Figure 2 below. This notional chart includes adding HSPD-12 authentication and authorization as a requirement for accessing all services—particularly for cloud services as well as mobile devices and capabilities. Under our framework, these services would be identified as external connections, and should therefore require strong authentication. The agencies would need to ensure adequate control measures are in place by requesting additional information for their providers. This would enable agencies to take full advantage of the efficiencies of commercially-available technical solutions in these areas while protecting against cyber-attacks by making use of the enhanced security features of Managed Trusted IP Service providers, who should work in conjunction with the cloud services providers. If this is not initiated through regular industry partnerships, the Federal government could make this a requirement on all contracting vehicles for these services.
Figure 2. Current and Proposed TIC Architectures

(a.) Current TIC Architecture

(b.) Proposed TIC Architecture
Additionally, the ISIMC should include a notional implementation plan that outlines the milestones to be achieved by enhancing their existing Plans of Action and Milestones. These plans should include new milestones to guide D/As as they implement our HSPD-12 solution in the new architecture.

Recommendation 2: FedRAMP’s JAB Should Require Penetration Testing among Cloud Service Providers

In its September 2013 report, the GAO also highlighted a lack of progress on testing and evaluation among Federal information security programs. To bolster Federal efforts in this area, we recommend that the General Services Administration (GSA) should lead the effort of FedRAMP’s JAB to require that all cloud providers undergo penetration testing after government applications and/or data services are implemented. This testing would be included as the next phase of certification by a certified third party that is capable of conducting such testing following established standards. The goal of this testing is to establish the degree of risk associated with adversary penetration attempts (with some degree of empirical data) and the ability of the provider to detect and prevent penetration. Industry and government must agree on these standards for testing. We recommend a procedure similar to, if not the same as, the Payment Card Industry Data Security Standard (PCI DSS) as outlined by the PCI Security Standards Council.

The PCI defines penetration tests in the following way:

*Penetration tests attempt to exploit vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application testing as well as controls and processes around the networks and applications, and occurs from both outside the network trying to come in (external testing) and from inside the network.*

Under the PCI DSS, vendors are required to execute penetration tests at least annually and “after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server)
is added to the environment.” The PCCI DSS requires that these penetration tests be executed at both the network layer and application layer.53

The JAB should also adopt the model contracting language included in Appendix 3 when issuing an RFP for cloud services. Using this language in each cloud contract will help agencies meet their responsibilities for privacy, data management, and cybersecurity. Lastly, the JAB should develop an agreed upon accountability matrix for responding to security issues by clearly delineating roles for identifying, containing and mitigating threats.

Recommendation 3: Use HSPD-12 Credentials to Validate Identity for Federal Employees

Before accessing cloud services, we recommend that Federal employees strengthen their authentication processes by employing an HSPD-12 credential or acceptable equivalent to validate users’ identities. This is consistent with OMB Directive M-06-16, which recommends that D/As “allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access.”54 The solution should also include authorization for services and data access. That is, the Federal government should allow access to their data and services according to users’ roles regardless of whether the services are internal on their own devices or external with a commercial cloud provider.

Recommendation 4: Cloud Service Providers Must Share Aggregate System Log Files with Federal Agencies under Continuous Diagnostics and Mitigation

The current continuous diagnostics and mitigation framework requests data from cloud service providers on the basis of asset ownership. Cloud providers are reluctant to share certain kinds of information with agency CIOs because a given “cloud” often has multiple tenants in addition to the agency in question, and sharing certain information could pose risks for other tenants. But the fact remains that if the Federal government is

---

54 http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2006/m06-16.pdf
to fully realize the benefits of the cloud while executing DHS’s goal of continuous diagnostics and mitigation, it requires specialized information. If cloud service providers were to share their aggregate system log files to the maximum extent practicable with Federal CIOs, agencies would then be able to incorporate them into their internal dashboards as well as the Federal dashboard that is maintained by DHS. The improved visibility of performance data would allow senior leaders to make better decisions about mitigating risks.

Recommendation 5: OMB and DHS Should Develop and Issue Effectiveness Metrics for IGs to Use in FISMA Reporting

A key recommendation from the GAO’s September 2013 report was for OMB and DHS to “develop metrics for inspectors general to report on the effectiveness of agency information security programs.”55 Incorporating metrics such as these into the FISMA reporting process is an important step in shifting from a “checklist” mentality to a risk-based approach to information security. Federal executives should use this simple formula to help them develop these metrics:

\[
    \text{Cybersecurity risk} = f \left( \frac{\text{Number of successful cyberattacks}}{\text{Sum of successful and failed cyberattacks}} \right)
\]

In our 2013 paper “Measuring What Matters”, we proposed a Cyber Risk Indicator concept that will provide agencies with a quantitative assessment of their exposure to a cyber-attack. This risk indicator weighs the performance of information systems and the maturity of attendant information security policies and processes according to organizational priorities. The risk indicator will yield an overall picture of the adequacy of the agency’s information security controls in the context of mission priorities. As a part of this process, the recommendations of the IGs should include specific steps for mitigating risks addressed by the indicator’s results. It will also allow agencies to measure their progress continuously and plan for improvements in their risk posture.

By aggregating the results of the information security risk management evaluation, IG evaluations will identify a Cyber Risk Indicator for each agency at least once a year. Rather than a subjective grade, this indicator would be a number determined by a

55 GAO, September 2013, p. 45.
formula. It would be used by the agency as well as by oversight entities such as OMB, DHS, GAO, and Congress to improve how risk is managed in an organization.\textsuperscript{56}

**Desired Outcomes**

By taking an integrated approach as outlined in this paper, we believe agencies will realize the full value of cloud services by delivering mission-based services more efficiently and at less cost. For example, if an agency decides to move their email services to a commercial cloud provider, the agency could improve service delivery and reliability. This would be achieved by the following:

- The end user employing, at a minimum, two-factor authentication through the agency’s directory services;
- The end user accessing their email located in the cloud-provided solution (accessing an external connection through a TIC); and
- Based on a specified time, the cloud provider sending the agency log files of all agency cloud operations (continuous diagnostics and monitoring).

If an agency has consolidated all of its email services, then it would also meet the goals set under the Data Center Consolidation Initiative.

3: Challenges in Implementing the Plan

Agency CIOs will face a number of challenges in transitioning from the current cloud security framework to one that more fully integrates existing cybersecurity initiatives. Some of these challenges are conversations to be had between the government and the private sector, while others—such as the rise of the “Bring Your Own Device” ecosystem—involve changes in consumer preferences that must be taken into account.

1. Extent of Penetration Testing.
Working in concert after implementation of agency services, industry and government can arrive at common definitions and jointly decide on which attributes will be used to determine the extent of penetration testing in the operating environment.

2. What to Include When Sharing Log Files
Second, agencies and commercial cloud service providers will have to arrive at a common understanding about whether and to what extent the cloud provider will share information about its log files with the agency. Sharing log files may assist Federal officials with performing analysis and mitigation of risks of their networks, but doing this may also inadvertently reveal information about other tenants on the cloud provider’s network. Government and the private sector must find a suitable solution that facilitates real-time security analysis and mitigation while also protecting the information and privacy of other cloud tenants.

3. Cybersecurity Risk and Associated Definitions
The third challenge derives from our contention that cybersecurity risk is a function of the percentage of successful cyber-attacks an organization experiences. Departments and agencies will need to clearly define what constitutes both an attempted and successful cyber-attack, and to identify the variables that influence cyber risk. The ISIMC should lead this effort.
4. The Rise of the “Bring Your Own Device” Ecosystem

Finally, a more long-term challenge is the rise of the “Bring Your Own Device” (BYOD) ecosystem. This trend shows no sign of abating. Federal employees who connect to their employer’s networks using their smartphones or tablets create more access points that must be secured. Agency CIOs and policymakers must either restrict the type and amount of work-related computing that employees can perform on their smartphones, or develop efficient policy solutions that enable Federal workers to take advantage of the convenience that these devices offer while not compromising the security of sensitive Federal information. Once the ISIMC has issued the initial integrated architectural documents as stated in this paper, additional efforts should be focused on the architecture needed to implement and sustain mobile computing.

Conclusion

As the Federal government pursues cloud computing to reduce costs and optimize IT asset use, it must also ensure that it is doing all it can to augment the security of Federal networks. Our “Safer in Cyberspace” paper seeks to accomplish this latter goal by integrating current cybersecurity practices as they relate to the cloud and recommending enhancements to identity management and continuous monitoring practices, among others. These recommendations span both the public and private sectors while not losing sight of the end user’s role. These recommendations will help the Federal government address one of the most pressing challenges to U.S. national security, bringing a secure future that much to reality.

57 http://www.whitehouse.gov/digitalgov/bring-your-own-device
Appendix 1: Defining the Cloud

Cloud computing is a model for enabling ubiquitous, 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.


Throughout this document, we will draw on the National Institute of Standards and Technology’s (NIST) definition of cloud computing:

NIST identifies on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service as the essential building blocks that make up cloud services. These concepts are explained further in the table below.

Software, development platforms, and technical infrastructure can all be offered through the cloud. Networks of cloud services can be open to the public, restricted to a private group, or some combination of the two.

<table>
<thead>
<tr>
<th>Table 1.1: The NIST Definition of Cloud Computing</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>On-demand self-service</strong>: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.</td>
</tr>
<tr>
<td><strong>Broad network access</strong>: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).</td>
</tr>
<tr>
<td><strong>Resource pooling</strong>: The provider’s computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.</td>
</tr>
<tr>
<td><strong>Rapid elasticity</strong>: Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.</td>
</tr>
<tr>
<td><strong>Measured service</strong>: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.</td>
</tr>
</tbody>
</table>

Appendix 2: Overview of “Cloud First”

The potential streamlining and cost-saving benefits of cloud computing has motivated the Federal government to identify the adoption of this technology as a high priority. In September 2009, then-Federal CIO, Vivek Kundra, first announced the Federal Cloud Computing Initiative (FCCI). The next step in the evolution of the FCCI was the release of the 25 Point Implementation Plan to Reform Federal Information Technology Management (“25 Point Plan”) in December 2010. Pointing to successful applications of cloud computing in the private sector, the 25 Point Plan mandated an immediate, Federal government-wide shift to a “Cloud First” policy in which the OMB will “require that agencies default to cloud-based solutions whenever a secure, reliable, cost-effective cloud option exists.” It set timelines for agency CIOs to identify three “must move” services for cloud migration and required the Federal CIO to publish a cloud strategy.

As mandated in the 25 Point Plan, Kundra published the Federal Cloud Computing Strategy (FCCS) in February 2011. The FCCS aims to accelerate the realization of the benefits of cloud computing by doing all of the following:

- Articulating the benefits, considerations, and trade-offs of cloud computing;
- Providing a decision framework and case examples to support agencies in migrating towards cloud computing;
- Highlighting cloud computing implementation resources; and
- Identifying Federal government activities and roles and responsibilities for catalyzing cloud adoption.

The General Services Administration’s (GSA) Federal Cloud Computing Program Management Office is in charge of the daily management of the FCCS. Other agency roles and responsibilities under the FCCS are summarized in the table on the next page.

Finally, several complementary programs have been established to support the Federal push for cloud adoption. During the initial FCCI roll-out in 2009, OMB launched

---

58 http://www.whitehouse.gov/blog/streaming-at-100-in-the-cloud/
Apps.gov, an online store where Federal agencies can browse and purchase cloud-based IT services. Later, the 25 Point Plan laid out the framework for what would eventually become the Federal Data Center Consolidation Initiative (FDCCI), a program that supports the Federal shift to cloud computing by targeting a minimum of 800 data center closures by 2015. In December 2011, the Federal Risk and Authorization Management Program (FedRAMP) was established to accelerate cloud adoption through a “do once, use many times” approach to cloud provider certification. By allowing agencies to re-use assessments and authorizations, it seeks to not only streamline the procurement process, but also to strengthen and standardize security requirements by applying baseline criteria to all cloud services. Finally, through the oversight authorities of the OMB, the PortfolioStat initiative “requires agencies to review IT spending in six areas: collaboration, unified communications, enterprise content management, search, reporting and analysis, and content creation.”

---

**Table 2.1: Roles and Responsibilities in the FCCS**

| **National Institute of Standards and Technology (NIST)** | will lead and collaborate with Federal, State, and local government agency CIOs, private sector experts, and international bodies to identify and prioritize cloud computing standards and guidance |
| **General Service Administration (GSA)** | will develop government-wide procurement vehicles and develop government-wide and cloud-based application solutions where needed |
| **Department of Homeland Security (DHS)** | will monitor operational security issues related to the cloud |
| **Agencies** | will be responsible for evaluating their sourcing strategies to fully consider cloud computing solutions |
| **Federal CIO Council** | will drive government-wide adoption of cloud, identify next-generation cloud technologies, and share best practices and reusable example analyses and templates |
| **The Office of Management and Budget (OMB)** | will coordinate activities across governance bodies, set overall cloud-related priorities, and provide guidance to agencies |


---

64 25 Point IT Implementation Plan (2010, p. 6).
65 [http://gsa.gov/portal/category/102375](http://gsa.gov/portal/category/102375)
Appendix 3: Model Language for Federal Cloud Contracts

Sample Contractual Language

Definitions

1. For purposes of this Agreement the phrase “Federal Data” means all text, numerical data, database records, media files, demographic information, search history, geolocation information, or any other data that travels over Federal technology networks or is accessed by government users or government contractors to [CLOUD SERVICE PROVIDER], or to which [CLOUD SERVICE PROVIDER] otherwise gains access as a direct result of the cloud services provided to the Federal department and/or agency (“Federal D/A”).

2. For purposes of this Agreement, the phrase “data mining or other processing” means the capturing, maintaining, scanning, indexing, sharing with third parties, or any other form of data analysis or processing of Federal data provided to [CLOUD SERVICE PROVIDER] by [FEDERAL D/A] pursuant to this Agreement. “Data mining or other processing” includes, but is not limited to, permitting access to Federal data to which [CLOUD SERVICE PROVIDER] gains access as a direct result of related services provided by [CLOUD SERVICE PROVIDER] which are not otherwise services covered by the terms of this Agreement.

Regulatory and Statutory Compliance

3. This agreement incorporates by reference the requirements of the Federal Information Security Management Act, the Cross-Agency Priority Cybersecurity Goals, and the relevant Office of Management and Budget directives, as in force as of the date of this Agreement and as may, from time to time hereafter, be amended. [CLOUD SERVICE PROVIDER] warrants that it has the technological capability to handle the policies and procedures outlined in these documents, statutes, and regulations.
Data Ownership

4. [FEDERAL D/A] retains full ownership of all Federal data provided to [CLOUD SERVICE PROVIDER] or to which [CLOUD SERVICE PROVIDER] otherwise gains access by operation of this Agreement. Upon expiration or termination of [FEDERAL D/A’S] use of the [CLOUD SERVICE], [FEDERAL D/A] may extract Federal data (and if [FEDERAL D/A] cannot so extract, then [CLOUD SERVICE PROVIDER] shall extract on [FEDERAL D/A’S] behalf), and [CLOUD SERVICE PROVIDER] will delete Federal data, in accordance with this agreement.

Data Mining

5. For the purposes of this Agreement the phrase “unauthorized use of Federal data” means the data mining or other processing of Federal data for unrelated commercial purposes, advertising or advertising-related purposes, or for any other purpose not explicitly authorized by [FEDERAL D/A] in this Agreement.

6. [CLOUD SERVICE PROVIDER] will take all reasonably feasible, physical, technical, administrative, and procedural measures to ensure that no unauthorized use of Federal data occurs. [CLOUD SERVICE PROVIDER] warrants that all active and latent technical capabilities to conduct data mining or other processing that would constitute an unauthorized use of Federal data have been either removed from its software package or disabled entirely.

7. Notwithstanding any provision of this Agreement, or any other agreement between the parties, or any published policy of [CLOUD SERVICE PROVIDER], the terms of this subsection take precedence over and replace any generally applicable privacy, data access or use, or similar policy of [CLOUD SERVICE PROVIDER], which the parties understand and hereby agree have no application to the processing of Federal data.

8. [CLOUD SERVICE PROVIDER] agrees and understands that implementation of this subsection may require it to modify or disable certain aspects of the software solution it proposes to provide to [FEDERAL D/A]. [CLOUD SERVICE PROVIDER] warrants that it has the technical capacity to implement the
technical changes required to conform to the requirements of this subsection. In particular, [CLOUD SERVICE PROVIDER] warrants that it can either disable completely or modify its software solution such that the applications services provided to [FEDERAL D/A] under this Agreement do not permit the unauthorized use of Federal data by other applications services provided by [CLOUD SERVICE PROVIDER] which are interoperable with the applications services provided under this Agreement.

Audit

9. [CLOUD SERVICE PROVIDER] will, upon the request of [FEDERAL D/A], provide either: (a) a reasonable ability to inspect [CLOUD SERVICE PROVIDER]'s handling of [FEDERAL D/A]'s data; or (b) the report of an expert, independent, third party, verifying compliance with the provisions of this Agreement.

Continuous Monitoring and Diagnostics

10. [CLOUD SERVICE PROVIDER] will provide aggregate system log files updating the [FEDERAL D/A] dashboard within eight hours of receiving new data through their internal processes and consistent with Security Content Automation Program (S-CAP) protocols.

Portability and Interoperability

11. [CLOUD SERVICE PROVIDER] will maintain Federal data provided to it by [FEDERAL D/A] in a format that, to the maximum extent practicable, permits the export of Federal data and the interoperable use of Federal data by other cloud service providers, to an extent that does not compromise the security and integrity of the data. To the extent practicable cloud applications and Federal data databases shall be maintained be in universally recognized formats.

Integrity

12. [CLOUD SERVICE PROVIDER] will maintain physical or logical separation between the cloud services provided to [FEDERAL D/A] and the consumer cloud services, if any, that it provides to other customers. [CLOUD SERVICE PROVIDER] will further ensure that there is no commingling of Federal data.
with data in [CLOUD SERVICE PROVIDER]’s consumer cloud services or with
data resulting from any data processing activities conducted by [CLOUD
SERVICE PROVIDER] as part of its consumer services. If the system is designed
to house evidentiary material, then the [CLOUD SERVICE PROVIDER] shall
maintain records of access to Federal data sufficient to allow [FEDERAL D/A] to
establish a chain of custody for data of evidentiary value.

General Provisions

13. The terms of this Agreement shall be binding on [CLOUD SERVICE PROVIDER]
and its legal successors and assignees.

14. [CLOUD SERVICE PROVIDER] expressly agrees that its failure to fully comply
with any provision of this Agreement will result in irreparable harm to
[FEDERAL D/A] and that [CLOUD SERVICE PROVIDER] shall be solely liable
for all reasonably foreseeable results of such failures, including, but not limited
to, unauthorized access to, or misuse of, Federal data, and that such failure shall
be cause for immediate termination of this Agreement, return of all Federal data
to [FEDERAL D/A], and [FEDERAL D/A]’s immediate exercise of any lawful
remedies.
Glossary

BYOD: Bring Your Own Device
CIO: Chief Information Officer
D/A: Department or Agency
FCCI: Federal Cloud Computing Initiative
FCCS: Federal Cloud Computing Strategy
FDCCI: Federal Data Center Consolidation Initiative
FISMA: Federal Information Security Management Act
GAO: Government Accountability Office
GSA: General Services Administration
IaaS: Infrastructure as a Service
IG: Inspector General
IT: Information Technology
NIST: National Institute of Standards and Technology
OMB: Office of Management and Budget
PaaS: Platform as a Service
PCI DSS: Payment Card Industry Data Security Standard
PII: Personally identifiable information
PIV Card: Personal Identification Verification Card
POAMs: Plans of Action and Milestones
About the Authors

Karen S. Evans serves as national director for the U.S. Cyber Challenge, a nationwide program focused specifically on the cyber workforce. She serves as a voice of authority for SafeGov.org, an online forum focused on cloud computing policy issues. She retired after nearly 28 years with the federal government, including service as administrator for e-government and information technology at the Office of Management and Budget, where she oversaw the federal information technology budget of nearly $71 billion.

Julie M. Anderson is a Managing Director at Civitas Group, a strategic advisory services firm in the national security markets. She also serves as an expert for SafeGov.org, an online forum focused on cloud computing policy issues. Recently, Ms. Anderson served as Acting Assistant Secretary for Policy and Planning and Deputy Assistant Secretary for Planning and Evaluation for the U.S. Department of Veterans Affairs (VA) in the Obama Administration. Prior to her appointment, Ms. Anderson worked for IBM’s Public Sector Global Business Services practice in Washington, D.C.

Brian D. Shevenaugh is an Associate with Civitas Group, where he supports the firm’s strategy and M&A practices. In this role, he provides research and analysis for engagements focused on market intelligence, strategy development and business alignment, and buy-side M&A strategy. He has supported engagements across the national security sector with specific areas of focus in defense and aerospace, cybersecurity, and government IT, including the SafeGov.org IT policy initiative. Previously, he performed media analyses, conducted tactical media relations, and researched sustainability issues with Edelman in Washington, D.C., and Chicago.