Executive Overview

The ability to embrace cloud computing capabilities for federal departments and agencies brings advantages and opportunities for increased efficiencies, cost savings, and green computing technologies. However, cloud computing also brings new risks and challenges to securely use cloud computing capabilities as good stewards of government data. In order to address these concerns, the U.S. Chief Information Officer (U.S. CIO) requested the Federal CIO Council launch a government-wide risk and authorization management program. This document describes a government-wide Federal Risk and Authorization Management Program (FedRAMP) to provide joint security assessment, authorizations and continuous monitoring of cloud computing services for all Federal Agencies to leverage.

Cloud computing is not a single capability, but a collection of essential characteristics that are manifested through various types of technology deployment and service models. A wide range of technologies fall under the title "cloud computing," and the complexity of their various implementations may result in confusion among program managers. The guidelines embraced in this document, represent a subset of the National Institute of Standards and Technology (NIST) definition of cloud computing, with three service models; Software as a Service, Platform as a Service, and Infrastructure as a Service (SaaS, PaaS, and IaaS).

The decision to embrace cloud computing technology is a risk-based decision, not a technology-based decision. As such, this decision from a risk management perspective requires inputs from all stakeholders, including the CIO, CISO, Office of General Counsel (OGC), privacy official and the program owner. Once the business decision has been made to move towards a cloud computing environment, agencies must then determine the appropriate manner for their security assessments and authorizations.

CLOUD COMPUTING AND GOVERNMENT-WIDE RISK AND AUTHORIZATION

Cloud Computing systems are hosted on large, multi-tenant infrastructures. This shared infrastructure provides the same boundaries and security protocols for each customer. In such an environment, completing the security assessment and authorization process separately by each customer is redundant. Instead, a government-wide risk and authorization program would enable providers and the program office to complete the security assessment and authorization process once and share the results with customer agencies.

Additionally, the Federal Information Security Management Act (FISMA) and NIST special publications provide Federal Agencies with guidance and framework needed to securely use cloud systems. However, interpretation and application of FISMA requirements and NIST Standards vary greatly from agency to agency. Not only do agencies have varying numbers of security requirements at or above the NIST baseline, many times additional requirements from multiple agencies are not compatible on the same system. A government-wide risk and authorization program for cloud computing would allow agencies to completely leverage the work of an already completed authorization or only require an agency to complete delta requirements (i.e. unique requirements for that individual agency).

Finally, security authorizations have become increasingly time-consuming and costly both for the Federal Government and private industry. As depicted in Figure 1, government-wide risk and

authorization program will promote faster and cost-effective acquisition of cloud computing systems by using an 'authorize once, use many' approach to leveraging security authorizations. Additionally, such a program will promote the Administration's goal of openness and transparency in government. All of the security requirements, processes, and templates will have to be made publicly available for consumption not only by Federal agencies but private vendors as well. This will allow Federal Agencies to leverage this work at their agency but private industry will also finally have the full picture of what a security authorization will entail prior to being in a contractual relationship with an agency.

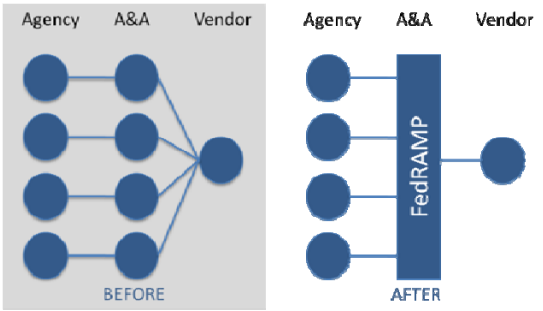

Figure 1: FedRAMP eliminates redundancy.

STANDARDIZED ASSESSMENT & AUTHORIZATION: FedRAMP

The Federal Risk and Authorization Management Program (FedRAMP) is designed to solve the security authorization problems highlighted by cloud computing. FedRAMP will provide a unified government-wide risk management process for cloud computing systems. FedRAMP will work in an open and transparent manner with Federal Agencies and private industry about the Assessment and Authorization process.

Through this government-wide approach, FedRAMP will enable agencies to either use or leverage authorizations with an:

- Interagency vetted approach using common security requirements;
- Consistent application of Federal security requirements;
- Consolidated risk management; and
- Increased effectiveness and management cost savings.

In addition, FedRAMP will work in collaboration with the CIO Council and Information Security and Identity Management Committee (ISIMC) to constantly refine and keep this document up to date with cloud computing security best practices. Separate from FedRAMP, ISIMC has developed guidance for agency use on the secure use of cloud computing in *Federal Security Guidelines for Cloud Computing*.

TRANSPARENT PATH FOR SECURE ADOPTION OF CLOUD COMPUTING

The security guidance and FedRAMP assessment and authorization process aims to develop robust cloud security governance for the Federal Government. The collective work that follows represents collaboration amongst security experts and representatives throughout government including all of the CIO Council Agencies.

By following the requirements and processes in this document, Federal agencies will be able to take advantage of cloud based solutions to provide more efficient and secure IT solutions when delivering products and services to its customers.