

Cloud Computing Security Standards

Evolving From the Classic Data Center Baseline

Government IT systems must meet significant statutory and regulatory requirements regarding security, security standards, and security practices. Historically, those IT assets had different types of controls placed on them, and security policies and procedures for in-house or contractor-operated systems were more immediately manageable. Moving to a Cloud Computing environment requires “rethinking” how to address IT systems security planning, policies, and procedures. Many of the standards in use industry-wide will need to change and evolve.

Cloud Computing is a “game changer” in information systems and cyber security.

Historically, cyber security issues largely focused on physical asset protection. Over the past two decades, much more attention has been paid to the systems themselves and the data they store and process to prevent malicious access and modification. In other cases, requirements address business, medical, and other types of personal information. Various pertinent laws include:

- Federal Information Security Management Act (FISMA) of 2003
- Children’s Online Privacy Protection Act of 1998
- Computer Matching and Privacy Protection Act of 1988 and Amendments of 1990
- Driver’s Privacy Protection Act of 1994
- Electronic Communications Privacy Act of 1986
- Health Insurance Portability and Accountability Act of 1996

Compliance with these regulations is not optional, and in many cases these regulations affect an agency’s partners, who are third-party stakeholders. For example, standards are promulgated from the US Department of Commerce with National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) publications and its SP-800 series on security. Individual agencies have promulgated their own standards, operationalizing the approach to security using federal standards as baselines. In some cases, the approach is modified to reflect the specific products and technology the agencies use or mission/community-specific requirements.

Many unknown factors exist for clients who are determining how they will incorporate Cloud Computing with their current operations. Concerns such as limited and evolving security standards and a general lack of established Cloud Computing governance make these decisions difficult for clients.

Booz Allen: beyond understanding is knowledge application

As a trusted advisor in this process, Booz Allen Hamilton, a leading strategy and technology consulting firm, brings a wealth of history solving complex issues. Our history combined with



About Booz Allen

Booz Allen Hamilton has been at the forefront of strategy and technology consulting for 95 years. Providing a broad range of services in strategy, operations, organization and change, information technology, systems engineering, and program management, Booz Allen is committed to delivering results that endure.

For more information contact

Drew Cohen

Vice President
301/543-4767
cohen_drew@bah.com

Michael Farber

Vice President
703/377-7780
farber_michael@bah.com

Mike Cameron

Principal
301/543-4432
cameron_mike@bah.com

Ron Ritchey

Principal
703/337-6704
ritchey_ronald@bah.com

www.boozallen.com/rfwn

For more information on the Booz Allen Hamilton CCW, please e-mail us at cloudcomputing@bah.com

Ready for what's next. www.boozallen.com/rfwn

Booz | Allen | Hamilton

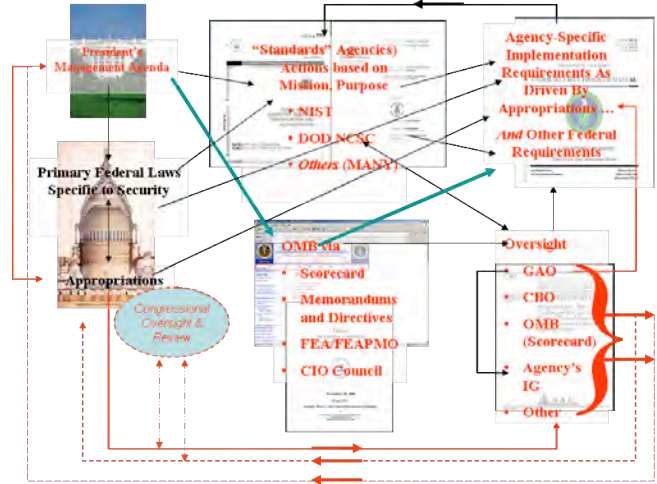
delivering results that endure

our ability to understand and implement complex security solutions allows us to offer our clients end-to-end assistance in identifying and solving their cloud security needs.

Booz Allen's extensive experience in cyber security, reinforced by our own Cloud Computing prototyping and customer pilot programs, positions us to provide a comprehensive analysis associated with moving to a cloud environment. Against the backdrop of complex and evolving governance issues, which public

law and events—such as the recently reported intrusion and personal information theft at the Federal Aviation Administration—often impel, Booz Allen's knowledge, expertise, and services become even more compelling resources.

US Government CyberSec "Governance" Model



Booz Allen's services yield verifiable results

Moving to the cloud requires asking and answering common questions regarding information systems security. However, other issues also arise, such as the integration of vendor assurance and resilience models and standards with internal plans and requirements, service-level agreement (SLA) management, plans and procedures, and incident monitoring and reporting. Agencies must plan for the cloud differently than conventional systems would warrant, and those differences are both vivid and subtle.

Booz Allen's security services span virtually all levels of security planning and requirements for government in the civilian and defense areas. Booz Allen ensures the viability of security in the cloud-based computing environment by providing tailored and adaptable tools and methodologies. Specifically, our approach focuses on five core areas of security: assessments, governance, engineering, operations, and training and awareness. By focusing on these core areas of security, we help our clients manage the security of their cloud environment from conception—not as an afterthought.

Booz Allen's staff of certified security experts assists clients in defining and developing their security strategy, vision, goals, objectives, and supporting policies and procedures. Our approach is based on the organization's business value proposition and current and envisioned operating environments. We work closely with the client organization to define a strategy that both supports achieving effective security and aligns with the overall business objectives. Critical to our approach is achieving consensus among key stakeholders regarding the cloud-based security strategy, standards, and operational models to reinforce the security policy and standards compliance. Without that consensus, no effort can be successful.

Once defined and approved, the Booz Allen implementation meets the standards and goals of technical and programmatic requirements from a cost/schedule/performance perspective, including O&M-centric services and capabilities, such as security change management capability programs and processes. Properly defined and applied standards will support operational and mission success in the Cloud Computing environment.

Whether you're managing today's issues or looking beyond the horizon, count on us to help you be ready for what's next.