Cloud Computing Security
Government Acquisition Considerations for the Public Cloud Computing Environments

by
Karen Mercedes Goertzel
goertzel_karen@bah.com
Holly Lynne M. Schmidt
schmidt_holly_lynne@bah.com
Theodore Winograd
winograd_theodore@bah.com
Kristy Mosteller
mosteller_kristy@bah.com

Booz | Allen | Hamilton
delivering results that endure
Table of Contents

Cloud Computing Security ................................................................. 1
Introduction ...................................................................................... 1
Purpose ............................................................................................ 1
Exclusions ........................................................................................ 1
Security Considerations in Government Acquisition of Public Cloud Services .................... 1
Relevant Acquisition Security Policy and Guidance ......................................................... 2
Supplier Selection ............................................................................. 2
Candidate Supplier Identification ............................................................ 2
Criteria for Choosing From Among Candidate Vendors ................................................. 4
Service–Level Agreements ...................................................................... 5
Standard Vendor Service–Level Agreements and Their Negotiability ................................. 5
Quality of Service and Quality of Protection Concerns .................................................... 7
Conclusion ........................................................................................ 7
About the Authors ............................................................................ 8
About Booz Allen ............................................................................... 9
Principal Offices ............................................................................... 10
Cloud Computing Security
Government Considerations for the Cloud Computing Environment

Introduction
Cloud computing is not a new technology or even a new computing paradigm. It is an umbrella term for a conceptual framework through which existing technologies, capabilities, computing concepts, provisioning, and charge-back approaches are more smoothly coordinated and integrated—often in ways that provide value far beyond each component in isolation. The “cloud” can also be seen as an abstraction mechanism, interposing one or more layers between the user and the systems that provide computing services and resources. These abstraction layers reduce or eliminate the end user's need to operate the mechanisms that make those services and resources accessible. Nevertheless, these same abstraction layers can make it difficult for the user to have any visibility into what happens to data or applications located “in the cloud.”

It is possible for U.S. government organizations to migrate desired services to a public cloud computing environment (CCE), but doing so requires that CCE consumers have a strong understanding of cloud technology's capabilities and limitations, evolving government security policies, and how an organization's security policies can be implemented and enforced while using a public CCE—as well as a comprehensive transition methodology, such as Booz Allen Hamilton's Cloud Computing transition Framework (C3F). An organization should have a planning effort that includes all acquisition and cloud expertise necessary, along with a clear realization that security is more than just a compliance activity. As they would with all responsible risk management decisions, government organizations should avoid allowing cost considerations to trump security considerations when deciding whether to acquire public cloud services, which type(s) of cloud services to acquire, and which cloud vendor(s) to trust with their data.

Purpose
This paper is intended to help the reader understand the information assurance (IA) and mission assurance (MA) challenges public CCEs pose and how accounting for those risks through acquisition security measures may affect public CCE options. It discusses security and risk management factors the Government should consider before acquiring public cloud services. For example, it outlines security criteria for evaluating different public CCEs and vendors, as well as the abilities and limitations of service-level agreements (SLA) and memoranda of agreement (MOA) with regard to risk.

Exclusions
The focus of this paper is solely on government acquisition and use of public cloud services. This paper does not address security issues associated with government organizations' implementation of private clouds or participation in community clouds operated by government agencies (e.g., Defense Information Systems Agency [DISA], National Aeronautics and Space Administration [NASA], Department of the Interior [DOI]).

Security Considerations in Government Acquisition of Public Cloud Services
Organizations must assess the viability of their infrastructure to adopt cloud-based services and should use a solid transition methodology that encompasses the transformation lifecycle. Through a strategic diagnostics session, the assessment should consider drivers, pain points, capabilities, stakeholders, mission risks, federal continuity compliance, continuity of operations planning (COOP), IT infrastructure resilience, and critical infrastructure protection. An acquisition will only be successful if the acquired service fully meets the organization's objectives. To this end, Booz Allen developed the C3F to support organizations migrating to the cloud. An understanding of relevant acquisition security policy and guidance will also help organizations carefully consider the impact of

transitioning assets from their current IT infrastructure to a public CCE.

Once an organization has fully analyzed and captured its CCE vision and strategy to transition its assets to the CCE, it can then assess its intellectual capital (IC) portfolio for CCE provider candidates and evaluate its options against the strategic diagnostic's findings by identifying suppliers, pinpointing and leveraging criteria to assess candidate suppliers, and assessing supplier accountability through SLAs or MOAs. These actions will promote provider transparency and ensure organizations understand the protections afforded their data.

**Relevant Acquisition Security Policy and Guidance**

Although the component services that comprise the cloud (e.g., time-sharing services, virtual machine hosting) are not new technologies, there is little security-relevant acquisition, policy, or guidance language for such services within the Federal Government. For that reason, there is little language available for reinterpretation and adaptation to public cloud use. Section 4.1 of Department of Defense Directive (DoDD) 8100.02, *Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)*, provides a number of security mandates to which any commercial wireless devices or networks integrated with or connected to a DoD network must conform. Although a public CCE cannot be considered a wireless network, the concepts within DoDD 8100.02 are relevant to any commercial network or devices connecting to DoD networks; it may be useful for government planners to review DoDD 8100.02 for language that can be adapted into a policy governing DoD public cloud use.

The National Institute of Standards and Technology (NIST) has published the *Draft NIST Working Definition of Cloud Computing v15 and Presentation on Effectively and Securely Using the Cloud Computing Paradigm v25*. NIST is also planning to publish cloud computing guidance, including security guidance, for federal agencies. This guidance will aim to promote the effective and secure use of the technology in government and industry through technical guidance and cloud computing standards.²

**Supplier Selection**

**Candidate Supplier Identification**

Depending on the type of service desired, organizations can choose from a wide range of cloud vendors—as well as vendors that offer cloud services but do not distinguish themselves as cloud vendors (e.g., hosting companies offering infrastructure as a service [IaaS] or platform as a service [PaaS]). One important aspect for organizations to consider when selecting a cloud vendor is that the concept of cloud services that meet government regulations or specific customer-driven security and privacy requirements is relatively new. Although current cloud SLAs tend to focus specifically on reliability and geographic location of data,³ it is likely that cloud vendors will follow in the footsteps of other service providers in introducing language to assuage security and privacy concerns.

**Public IaaS Vendors**

**Exhibit 1 | Examples of IaaS Applications**

<table>
<thead>
<tr>
<th>IaaS Vendors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Web Services (AWS)</td>
</tr>
<tr>
<td>Engine Yard</td>
</tr>
<tr>
<td>Joyent</td>
</tr>
<tr>
<td>Mosso</td>
</tr>
<tr>
<td>FlexiScale</td>
</tr>
<tr>
<td>GoGrid</td>
</tr>
<tr>
<td>ElasticHosts</td>
</tr>
<tr>
<td>Terremark</td>
</tr>
<tr>
<td>Savvis</td>
</tr>
</tbody>
</table>

**Infrastructure**

Infrastructure comprises the hardware, networking, and operating systems that run the foundation of an information system. This infrastructure includes fiber optic cables, hard drives, servers, and usually an

---


operating system. From the perspective of a software developer, this infrastructure runs the code that produces the screens, data, and workflows the end users interact with, but the infrastructure is not the code itself. In short, IaaS abstracts a particular type of hardware with a stack (e.g., Windows, Linux, other operating system), as well as one or two databases and networking support.

The basic principle on which IaaS stands is the multiplexing of resources among many users to increase average utilization. Users are able to allocate and de-allocate virtual servers from a virtual pool on demand, providing users with elasticity that is generally unavailable in traditional computing models. To support IaaS, organizations agree to have their virtual servers potentially co-located with other organizations’ servers on the same physical platform—this is similar in concept to virtual servers that can be provisioned from commercial hosting providers. Although the logical separation provided by the IaaS vendor is usually sufficient, the act of co-locating data on a single physical platform may make it a more valuable target for attackers.

It is important to note that although the cloud vendor provides some security controls, these controls are only at the infrastructure level, conceptually below the virtual operating system presented to the customer. The customer may place additional software-based controls on the virtual server (provided the controls do not violate the cloud vendor’s terms of use) to help secure organizational data and processes that will be hosted on the cloud.

**Public PaaS Vendors**

A cloud PaaS—which is the delivery of a computing platform and/or solution stack as a service—facilitates the deployment of applications without the cost and complexity of buying and managing the underlying hardware and software layers.

It is important to note that, as with IaaS vendors, the cloud vendor provides the security controls in place below the base platform and APIs presented to the customer. The customer may place additional software-based controls on the application or service to help secure organizational data and processes that will be hosted on the cloud. For example, the web application or service can be developed to process anonymous or generic data that can be correlated to the original data when it is returned to the organization’s boundary.

---

**Exhibit 2 | Examples of PaaS Applications**

<table>
<thead>
<tr>
<th>PaaS Vendors</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google App Engine</td>
<td>Provides the base platform and application programming interfaces (API) for developing and deploying Python and Java-based web applications and web services</td>
</tr>
<tr>
<td>Microsoft Azure</td>
<td>Provides the base platform and APIs for developing and deploying .NET-based web applications and web services</td>
</tr>
<tr>
<td>Morph</td>
<td>Provides the Morph Application Platform for developing web applications</td>
</tr>
<tr>
<td>Heroku</td>
<td>Provides the base platform and APIs for developing and deploying Ruby on Rails-based web applications and web services</td>
</tr>
<tr>
<td>Bungee</td>
<td>Provides an IDE and platform for developing and deploying web applications and web services</td>
</tr>
</tbody>
</table>
Public Software as a Service (SaaS) and Data as a Service (DaaS)\(^\text{4}\) Providers

### Exhibit 3 | Examples of SaaS Applications

<table>
<thead>
<tr>
<th>PaaS Vendors</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Apps</td>
<td>Offers a suite of office products through the cloud for customers to use</td>
</tr>
<tr>
<td>AWS</td>
<td>Offers a number of service APIs that can be used to extend the capabilities of an organization’s software</td>
</tr>
<tr>
<td>SAP</td>
<td>Provides the same functionality as its commercial off-the-shelf (COTS) offering through a subscription model via the cloud</td>
</tr>
<tr>
<td>Salesforce.com</td>
<td>Provides the same functionality as its COTS offering through a subscription model via the cloud</td>
</tr>
<tr>
<td>Microsoft Azure</td>
<td>Offers a number of service APIs that can integrate with both thin and thick clients on users’ computers</td>
</tr>
</tbody>
</table>

A cloud SaaS leverages the cloud in software architecture, often eliminating the need to install and run the application on the customer’s own computer and thus alleviating the burden of software maintenance, ongoing operation, and support. A cloud SaaS includes “products, services and solutions that are delivered and consumed in real-time over the Internet,”\(^\text{5}\) such as web services (“software system[s] designed to support interoperable machine-to-machine interaction over a network.”\(^\text{6}\)). Other cloud computing components, software (e.g., software plus services), or end users may directly access a SaaS. Cloud data storage services (DaaS) involve the delivery of data storage as a service, including database-like services. DaaS is often billed on a utility computing basis (e.g., per gigabyte per month).

It is important to note that the cloud vendor provides the security controls in place for the entire software stack presented to the customer. The customer may place additional controls between the user and the application (i.e., anonymizing data before submitting it to the service) to help secure organizational data and processes that will be hosted on the cloud. However, for SaaS and DaaS offerings, organizations must trust that the vendor’s security controls are sufficient to protect the entire software stack. With SaaS and DaaS services in particular, cloud vendors may be unwilling to modify their security practices, particularly when a COTS version of the software in the SaaS or DaaS service offering can be deployed and secured at a customer’s organization.

### Security Concerns Common Across All Cloud Services

The primary concern associated with cloud offerings is that customer data is stored offsite at the vendor’s data centers and therefore must be protected by the vendor’s security controls. An additional concern with cloud offerings is that the data from multiple customers is potentially co-located in one facility—increasing the value of the data stored at the center. Although many vendors provide customers thorough descriptions of their existing security controls, few vendors—if any—allow customers to perform a detailed audit of their security controls and standards. In addition, few cloud vendors are willing to modify their security controls for cloud offerings at a customer’s request.

### Criteria for Choosing From Among Candidate Vendors

As with selecting a supplier for any IT service, the first and foremost criterion for provider selection

---

\(^{\text{4}}\) NIST does not formally recognize the terminology “Data as a Service (DaaS)” as a defined service in its cloud computing documentation; however, it is phrased as such in this paper for consistency and ease of readability


must be whether the vendor meets the organization’s needs. For example, one CCE provider may be willing to provide security controls that exceed customer requirements while also allowing the organization to audit the provider’s security practices, but the services offered by the provider may not fit correctly with the organization’s business processes or expectations. In such situations, simply choosing a CCE provider based on the security and privacy assurances it provides would not meet the needs of the organization.

As with any acquisition, it may be necessary to make some compromises in terms of requirements to meet the organization’s needs—but it is of utmost importance that such decisions are made with a full understanding of their potential consequences. When choosing between candidate suppliers, it is important to use security and auditing practices as distinguishing factors in addition to price, performance, and other factors.

**Service-Level Agreements**

SLAs represent both a source of security risk in public CCEs and a means of addressing security risk. The SLA is the main means by which the cloud consumer can mitigate the security risks that this shift of operational responsibility engenders. To address the consumer’s lack of visibility, lack of control, and lack of accountability, the SLA can explicitly state the security requirements of the cloud customer, including requirements for service quality and availability, MA, data confidentiality and privacy, data and software integrity, incident response, vulnerability management, and problem resolution.

As providers of a “commodity” service, many public CCE providers tend to standardize their SLAs for all of their customers. SLA standardization can introduce risk by failing to address and accommodate the specific security requirements of individual customers. In the absence of an SLA that satisfies all of a customer’s requirements, that customer will need to negotiate with the provider to tailor the SLA to satisfy the organization’s needs; otherwise, the organization will need to find alternative means by which to minimize residual risk. Some of the leading public CCE providers recognize a need to meet their customers halfway in order for widespread public CCE adoption to occur. For example, Amazon has begun offering “virtual private cloud” services that combine the outsourcing advantages of the public cloud with increased customer visibility, control, and service tailoring (at a cost higher than that of Amazon’s fully public Elastic Compute Cloud [EC2] cloud service). But for many customers, the perceived cost savings associated with using public CCEs offered under less-than-ideal standard SLA terms will outweigh the potential losses associated with the increased risk that accompanies the acceptance of such terms.

The key to success is setting realistic expectations from the outset so that all stakeholders in the acquiring organization understand the exact level of service their public cloud provider is willing to provide. If the SLA meets the performance/availability/reliability (PAR) needs of the organization, the cost-benefit analysis is usually clear (keeping in mind that PAR must explicitly include all of the customer’s security considerations). If the SLA falls short, organizations should factor the quantified level of risk associated with the shortfall into the cost-benefit equation.

**Standard Vendor Service-Level Agreements and Their Negotiability**

SLAs are not a new concept for service providers or the customers that purchase them. Customers should apply the same SLA standards in a CCE that they would in an outsourcing requirement. When entering the tenuous nature of the cloud, however, customers must be increasingly vigilant in assessing their needs, what they are or are not willing to negotiate, and the price they are willing to pay for guarantees and assurances. As a customer, the key is to annotate the organization’s nonnegotiable needs as the baseline price point and proceed from there. At a minimum, the SLA should include details about asset ownership, downtime, customer service, and pricing. Organizations should be familiar with common language used in the CCE, as well as standard SLA language. Combined, this language creates an agreement that may differ...
from an organization’s understanding of typical SLA terminology. Larger scale providers typically use more generic language to encompass broader capabilities and to relieve the organization’s (i.e., the customer’s) responsibility. It is the organization’s responsibility to ensure the SLA expressly identifies and defines specific issues and desired services.

**Data Ownership and Control**

Organizations should ensure the SLA clearly defines who has access to the data and the protections that are in place. The customer’s data and IT managers will need to understand how the provider’s infrastructure and services are used to provide persistent access to needed applications and data sets. Continuity is important. In a perfect world, a vendor could guarantee access 100 percent of the time, but, in reality, a guarantee like that is impossible. The customer’s legal department needs to understand the differences between common SLA terms such as “average configuration downtime” or “network downtime” versus “systems downtime.” Organizations should also have a clear definition of who owns the data and should consider self-protecting data options as necessary.

**Auditing and Accountability**

Although most cloud providers will record access to the system in specified log files, gaining access to audit logs can be a difficult process. In some instances, the cloud provider’s logs may be insufficient for a particular organization’s needs. To this end, organizations are often forced to run their production applications on an implicit SLA that is usually interpreted as a simple equation of receiving X units of service for N price. Unfortunately, this implicit SLA does not address the scalability of an organization’s resources based on changes in demand. Auditing becomes another key factor in assessing the organization’s true needs and being able to meet ever-changing demands in service. Instead of accepting what the CCE provider sends the organization at the end of the month as a bill, an organization should understand that cloud computing is complex enough that a reasonable set of runtime information must be made available to substantiate the provider’s claim for compensation.

This point is particularly true in developing an SLA. If the organization’s infrastructure is regularly adjusting to meet demands, it is essential to be able to verify that the infrastructure is reacting the way that was contracted. To complicate matters further, CCEs—which are innately self-service and on demand—create a plethora of data to be maintained and filtered. For this reason, SLAs with providers should explicitly state that real-time auditing or logging (for accountability) will be performed and resulting reports will be made accessible to customers. A tailored audit can provide the customer a clear understanding of where responsibilities lie.

**Compliance Environments**

Compliance environments cited by experts as important for cloud computing include Statement on Auditing Standard (SAS) 70, Payment Card Industry Data Security Standards (PCI DSS), and the Health Insurance Portability and Accountability Act (HIPAA). In particular, experts cite the section in SAS 70 on Service Organizations issued by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA). Basically stated, the vendor managing the cloud must be able to describe what is happening, where the information comes in, what the vendor does when it gets the information, how it gets back to the users, the controls over the processing of the data, and, most importantly, what is happening to the data when it gets to the cloud.

Although many public CCE providers have SAS 70 or even PCI compliance, many do not fully address NIST Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems and Organizations. SP 800-53 outlines the security controls expected of federal government organizations. Although many cloud providers lack a full understanding of recommended security controls, some cloud providers trying to pursue the government market are adequately complying with NIST SP 800-53. When assessing a provider, organizations should consider the following:

---

Is the provider familiar with federal requirements? Are the security controls the CCE provider is responsible for compliant? How does the CCE provider display evidence of compliance? How is compliance maintained?

Quality of Service and Quality of Protection Concerns
Public cloud service SLAs must account for at least two vendors: (1) the cloud service provider and (2) the communications vendor that provides the circuit by which the customer accesses the cloud service. This dual-provider scenario adds complexity to not only the SLA language but also the ability to hold vendors accountable (and legally liable) for failures. In addition, organizations must acknowledge that all service providers will experience downtime at some point because of situations beyond their control, including natural disasters and interruptions in the public infrastructure. Most service providers offer an assurance of 99.5-percent uptime. Even with expected legalese, a provider can make a reasonable attempt to guarantee an acceptable level of service.

With that in mind, the real question becomes the following: What happens when service is interrupted? Some providers have established mechanisms to assist organizations in assessing the quality of service (QoS) they are receiving and to inform organizations of any potential downtime or service disruptions. Although these mechanisms do not mitigate the actual loss of time or data, they can be used to prepare preventative and contingency measures after an SLA has been established. The bottom line in addressing sustainment issues is an organization’s ownership of risk. Using available resources to monitor the health of a provider’s service capabilities (as available) is one viable option; however, if an organization is clear in its expectations early on and develops appropriate SLA language, it will enjoy greater business continuity assurance.

Conclusion
Public CCEs are a potentially viable option for government organizations as an alternative to government ownership and operation of IT infrastructure and systems. However, government agencies must recognize that many security-related issues surround such a move. Before a government organization migrates some or all of its data to a public CCE, it must have a clear grasp of cloud technology and emerging government policies, as well as a comprehensive transition methodology, such as Booz Allen’s C3F. Moreover, it must realize that public CCE providers may not meet federal standards for security controls and may not be able to provide government organizations the requisite security measures. Government acquirers of public CCEs need to be fully aware of the security risks associated with the different public cloud service operating models (e.g., IaaS, PaaS, SaaS), as well as how the use of a particular model will affect the organization’s ability to maintain its mission.

As a cloud technology expert with deep knowledge of related government standards, Booz Allen can help clients navigate the new and complex cloud environment. Booz Allen addresses the challenges of the public cloud with an objective understanding of the security issues the cloud presents. To fully address all facets of a potential move to the cloud, Booz Allen offers the C3F to address the need for government organizations to have a trusted, unbiased advisor on their side as they determine whether to take this next step in computing. Through the C3F, Booz Allen’s consultants assist organizations with mission assessment, potential solution evaluation, requirements development, vendor selection, and, ultimately, acquisition. Booz Allen can also help organizations ensure their provider SLAs and MOAs are comprehensive and will protect them in any situation. With appropriate security-aware acquisition practices, government customers of public cloud services can decrease their security risks by moving to the cloud.

About the Authors

Karen Mercedes Goertzel, CISSP, is an Associate in Booz Allen Hamilton’s McLean office and currently leads the firm’s security research service. She is a subject matter expert in software security and safety assurance, cyber security, information assurance, and software system survivability.

Holly Lynne M. Schmidt, SSCP, CSSLP, is an Associate in Booz Allen Hamilton’s McLean office. She specializes in application security; system/software assurance; and security policy, law, and regulation. She has performed research, analysis, and development of reports, guidance, and policy for various government clients.

Theodore Winograd, CISSP, is an Associate in Booz Allen Hamilton’s McLean office. He specializes in information and software assurance, concentrating on service-oriented architecture and, more recently, cloud computing technologies.

Kristy Mosteller is an Associate in Booz Allen Hamilton’s One Dulles office. She specializes in system security engineering development and delivery, concentrating on security management, information technology, and operations risk analysis.

Contact Information:

Karen Mercedes Goertzel, CISSP
Associate
goertzel_karen@bah.com
703/698-7454

Holly Lynne M. Schmidt, SSCP, CSSLP
Associate
schmidt_holly_lynnne@bah.com
703/377-5547

Theodore Winograd, CISSP
Associate
author@bah.com
703/377-5544

Kristy Mosteller
Associate
author@bah.com
703/984-7085
About Booz Allen

Booz Allen Hamilton has been at the forefront of strategy and technology consulting for 95 years. Every day, government agencies, institutions, corporations, and not-for-profit organizations rely on the firm’s expertise and objectivity, and on the combined capabilities and dedication of our exceptional people to find solutions and seize opportunities. We combine a consultant’s unique problem-solving orientation with deep technical knowledge and strong execution to help clients achieve success in their most critical missions. 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.

With more than 22,000 people and $4.5 billion in annual revenue, Booz Allen is continually recognized for its quality work and corporate culture. In 2009, for the fifth consecutive year, Fortune magazine named Booz Allen one of “The 100 Best Companies to Work For,” and Working Mother magazine has ranked the firm among its “100 Best Companies for Working Mothers” annually since 1999.

To learn more about the firm and to download digital versions of this article and other Booz Allen Hamilton publications, visit www.boozallen.com.
### Principal Offices

<table>
<thead>
<tr>
<th>ALABAMA</th>
<th>KANSAS</th>
<th>OHIO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Huntsville</td>
<td>Leavenworth</td>
<td>Dayton</td>
</tr>
<tr>
<td>CALIFORNIA</td>
<td>MARYLAND</td>
<td>PENNSYLVANIA</td>
</tr>
<tr>
<td>Los Angeles</td>
<td>Aberdeen</td>
<td>Philadelphia</td>
</tr>
<tr>
<td>San Diego</td>
<td>Annapolis Junction</td>
<td></td>
</tr>
<tr>
<td>San Francisco</td>
<td>Lexington Park</td>
<td></td>
</tr>
<tr>
<td>COLORADO</td>
<td>Linthicum</td>
<td>SOUTH CAROLINA</td>
</tr>
<tr>
<td>Colorado Springs</td>
<td>Rockville</td>
<td>Charleston</td>
</tr>
<tr>
<td>Denver</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FLORIDA</td>
<td>MICHIGAN</td>
<td>TEXAS</td>
</tr>
<tr>
<td>Pensacola</td>
<td>Troy</td>
<td>Houston</td>
</tr>
<tr>
<td>Sarasota</td>
<td></td>
<td>San Antonio</td>
</tr>
<tr>
<td>Tampa</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GEORGIA</td>
<td>NEBRASKA</td>
<td>VIRGINIA</td>
</tr>
<tr>
<td>Atlanta</td>
<td>Omaha</td>
<td>Arlington</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Chantilly</td>
</tr>
<tr>
<td>HAWAII</td>
<td>NEW JERSEY</td>
<td>Falls Church</td>
</tr>
<tr>
<td>Honolulu</td>
<td>Eatontown</td>
<td>Herndon</td>
</tr>
<tr>
<td></td>
<td></td>
<td>McLean</td>
</tr>
<tr>
<td>ILLINOIS</td>
<td></td>
<td>Norfolk</td>
</tr>
<tr>
<td>O’Fallon</td>
<td></td>
<td>Stafford</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WASHINGTON, DC</td>
</tr>
</tbody>
</table>

*The most complete, recent list of offices and their addresses and telephone numbers can be found on www.boozallen.com by clicking the “Offices” link under “About Booz Allen.”*