Booz | Allen | Hamilton

Organizational Network Analysis

Improving Intelligence and Information Sharing Capability among Homeland Security and Emergency Management Stakeholders

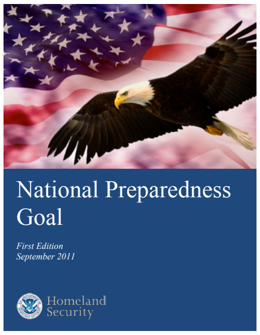
by

Christopher P. Bell
bell_christopher_p@bah.com

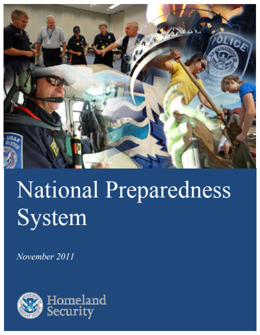
Elizabeth Conjar
conjar_elizabeth@bah.com

Organizational Network Analysis

Introduction



Our nation faces a wide range of threats and hazards, including acts of terrorism, pandemics, and natural disasters. Overcoming each of these threats requires coordination and collaboration among the full range of community partners: individuals, families, communities, private and nonprofit sectors, faith-based organizations, and all levels of government. No single level of government or organization has responsibility; it requires the combined efforts of the whole community.



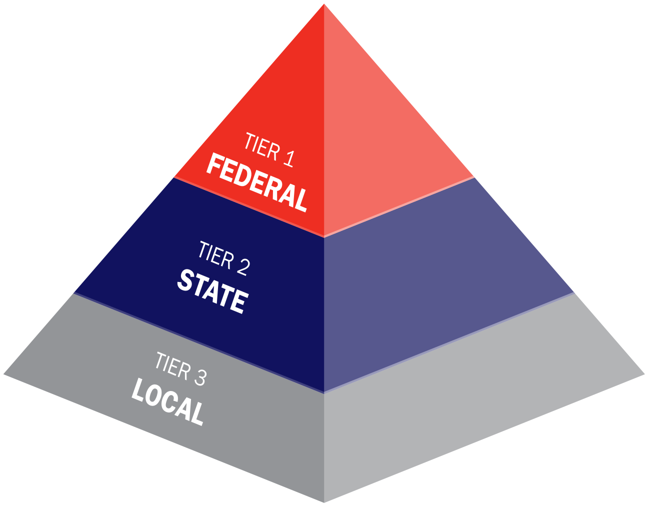
In March 2011, the President released Presidential Policy Directive 8 (PPD-8) describing the nation's approach to preparing for the threats and hazards that pose the greatest risk to the security of the United States. In November 2011, the Department of Homeland Security (DHS) released the National Preparedness Goal, which lays out the core capabilities needed for each of the missions areas: prevention, protection, mitigation, response, and recovery. The National Planning System was created to support the delivery of the core capabilities identified in the National Preparedness Goal. As a part of the National Preparedness System, a set of coordinated National Frameworks were developed for each of the mission areas that focuses on how the whole community prepares to deliver each of the core capabilities. Each Framework describes the coordinating structures and alignment of key roles and responsibilities for the whole community and is integrated to ensure interoperability across all mission areas.

Understanding Existing Intelligence and Information Sharing Networks

Booz Allen Hamilton, a leading strategy and technology consulting firm, understands that networks of intelligence and information sharing exist at all levels of government, and that they each coordinate with each other and other relevant stakeholders. There are numerous federal agencies providing technical advice, doctrine, and funding for state and local jurisdictions to stand up and maintain emergency operations centers and fusion centers throughout the country. In addition, numerous federal agency representatives located throughout the country coordinate and collaborate with state and local stakeholders regarding the processes and the mechanisms of intelligence and information sharing.

Current doctrine and guidance given by homeland security and emergency management communities provides a framework for intelligence and information sharing among stakeholders. As illustrated in Exhibit 1, the current approach provides stakeholders with a template of formal communication channels based

Exhibit 1 | Current Communication Framework



Source: Booz Allen Hamilton

on hierarchical charts or "planned communication" maps. In other words, current doctrine emphasizes communications that *should* occur on a routine basis or during a crisis. While beneficial for formal planning efforts, this approach fails to recognize the actual communication and collaboration network at work. The current approach does not provide the complete picture, allow stakeholders to diagnose current issues, or pinpoint successful relationships in the network. It also fails to recognize and capitalize on communications that emerge outside of doctrinal mandates—often through peer-to-peer contacts—that enable hidden efficiencies and resilience in peripheral regions of the network. The ability of the homeland security and emergency management communities to respond to a threat or an actual terrorist incident is in part dependent on the strength and effectiveness of its social networks. Consequently, understanding the interactions within and between security partners in relevant networks promotes situational awareness, coordinated planning, and optimal allocation of resources during prevention, protection, response, and recovery phases. Building resiliency into these networks requires an understanding of how networks evolve during normal times (routine communications), and during times of stress (communications related to a crisis scenario). Understanding how networks change when stressed and how to promote positive changes that allow networks to effectively communicate and/or respond is a key area in enhancing resilience.

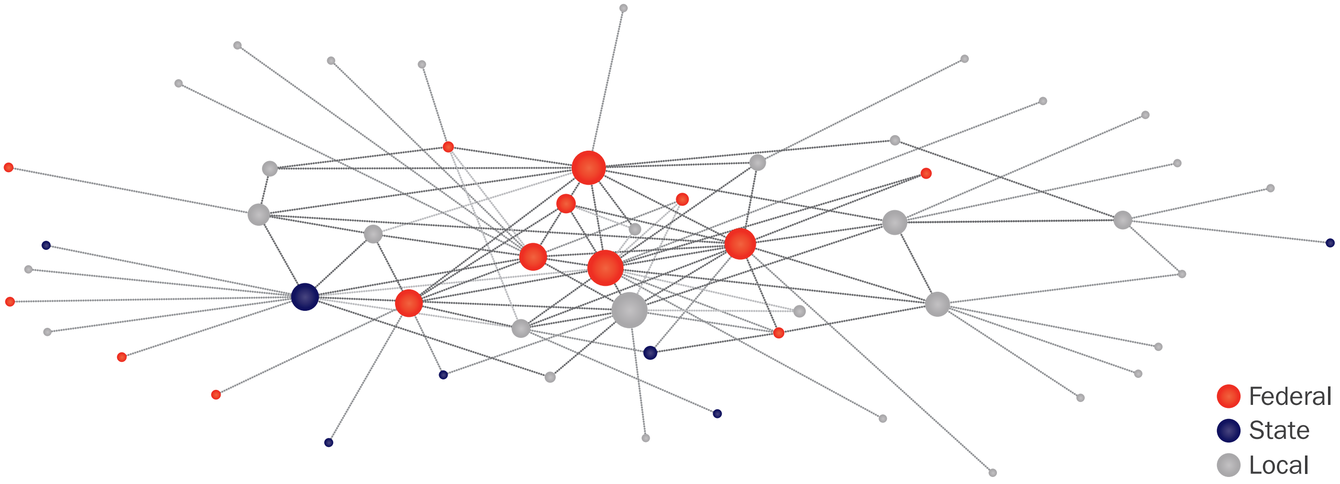
Empowering Stakeholders with Organizational Network Analysis

Organizational Network Analysis (ONA) offers a different perspective on organizational relationships. Network analysis techniques map actual communications occurring in the network, regardless of formal hierarchies, mechanisms for collaboration, organizational policies, and areas of responsibility.

ONA can be defined as the study of complex human systems through the mapping and analysis of social relationships between people, groups, and/or organizations. As a result, network maps and diagrams created from ONA look different from "planned communications" maps. As illustrated in Exhibit 2, ONA diagrams reveal how organizations communicate and collaborate irrespective of formal structures or geographic/demographic boundaries. ONA allows stakeholders to visualize and measure the invisible, informal networks that reflect how work really gets completed.

This methodology empowers stakeholders with the knowledge to make decisions related to security

Exhibit 2 | Communication Framework Using ONA



Source: Booz Allen Hamilton

partner communication and collaboration on both a routine and non-routine basis. For example, ONA reveals the characteristics, composition, and structure of existing networks in order to:

- Identify how flexibility could be built into networks or organizations.
- Determine the needed balance between efficiency and redundancy when building resilient networks.
- Identify sustainable linkages.
- Reveal new ways to coordinate personnel, resources, and information to improve response.

Employing network analysis is not a new concept at DHS, which has successfully used analytical tools to study external relationships—most notably in the study of terrorist networks that threaten the homeland. Just as important is developing an understanding of the complex internal connections and relationships within the emergency management and homeland security communities. ONA represents a unique approach to study and refine the communications and information flow in order to build resiliency across the public and private sectors.

Data Collection, Visualization, and Analysis

ONA data are most commonly collected through short, web-based surveys. Unlike most workplace surveys that focus on respondents' opinions about policies, activities, or resources, ONA surveys focus on understanding the relations between individuals or organizations. Respondents are asked questions about how their organizations connect to other organizations in relevant ways. The specific items (e.g., types of relations, list of organizations) in the survey are based on the context of the ONA effort, but typically will include communication, coordination, and dependency relations. By collecting the set of relations within and between organizations, we are able to construct networks for visualization and analysis.

Just as viewing a map can enable emergency managers to understand and communicate the "big picture" of a situation, network diagrams can quickly orient analysts and stakeholders to a network's key characteristics, including features such as:

- Distinct dense clusters representing highly connected sets of organizations.
- Weakly connected, or disconnected subgroups representing potential stovepipes or points of vulnerability.
- Key organizations that sit between large numbers of otherwise disconnected organizations, representing key information brokers and/or potential bottlenecks.

Moving beyond visualizations, network analysts can calculate a number of quantitative metrics to highlight important regions or individual organizations in a network. Just as statistics such as population density, demographics, or number of hospital beds in an area can provide insight to an emergency manager, network metrics can be used to measure the resilience and redundancy in a network, identify organizations that play key roles, or characterize organizations that are not fully integrated into the network. By combining powerful visualizations and quantitative measures, network analysts and stakeholders can quickly identify and orient to the strengths and weaknesses in an emergency response network.

Stakeholder Analysis

ONA results can empower stakeholders with the knowledge to make decisions related to improving communication and collaboration. Stakeholder analysis identifies the roles individuals or organizations play in their network, revealing their influence and power in the network. Stakeholder analysis can be broken down by important attributes to find general trends and make comparisons across sub-groups, such as federal, state, local, private sector, or regionally within the network. Further, it allows for comparison and validation of formal organizational roles of nodes. As illustrated in Exhibit 3, Stakeholder analysis typically identifies three key characteristic roles: (1) core connector, (2) bridge connector, and (3) peripheral connector.

Core Connector

As a core connector, an organization or individual is connected to a large number of other organizations through the relationship of interest (e.g., communication, collaboration). A typical example of a core connector would be a fusion center or an emergency operations center.

A very simple, but often effective measure of an organization's influence and command is its status as a core connector. Core connectors are significantly embedded in the inter-organizational network, and may be critical to many systems that keep network functioning effectively. They may have alternative ways to satisfy needs, and hence are less dependent on others in the network. They may also have access to, and be able to call on more of the resources of the network as a whole, in both routine and non-routine situations. Additionally, core connectors may represent nodes that have structures or policies in place that easily allow inter-organizational relationships, acting as a model for other organizations who have yet to develop such structures.

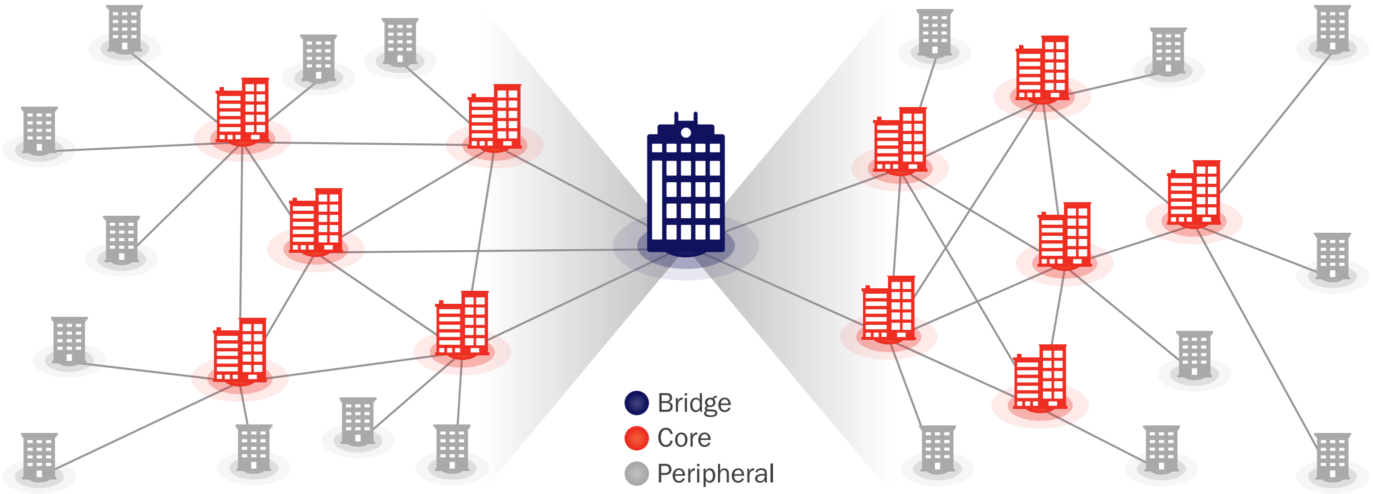
Bridge Connector

As a bridge connector, an organization or individual that controls the flow of information between other organizations in the network. Bridge connectors often act as intermediary partners, sending information or exchanging resources between disconnected parties that do not have direct relational connections to each other. A typical example of a bridge connector would be a private sector liaison or a critical infrastructure working group. Bridge connectors typically have the ability to drive response, assist in coordination, and diffuse information quickly throughout the network. Given their connections to other organizations or individuals that do not have connections to one another, bridge connectors have a large amount of influence over the information that does, and does not, flow through the network. They may act as a single point of failure in the network or as bottlenecks, slowing down or hindering communication and collaboration.

Peripheral Connector

As a peripheral connector, an organization or individual that sits on the edge of the network. Peripheral nodes related to organizational networks may be focused on very narrow initiatives or specific tasks, be less well known in the network, or may play a less critical role in information or resource sharing in an organizational network. A typical example of a peripheral connector would be a private sector transportation partners or

Exhibit 3 | Stakeholder Analysis Key Characteristics



Source: Booz Allen Hamilton

corporate security partners. Identification of peripheral players allows for an examination of organizations or individuals that are not significantly embedded into the network and can reveal if stakeholders need to take further action. It is possible that organizations, given their roles, should be found on the periphery of the network. ONA allows stakeholders to assess identified periphery connectors to determine if they are in the correct role, or if they are being over or under used.

Understanding the Whole Network

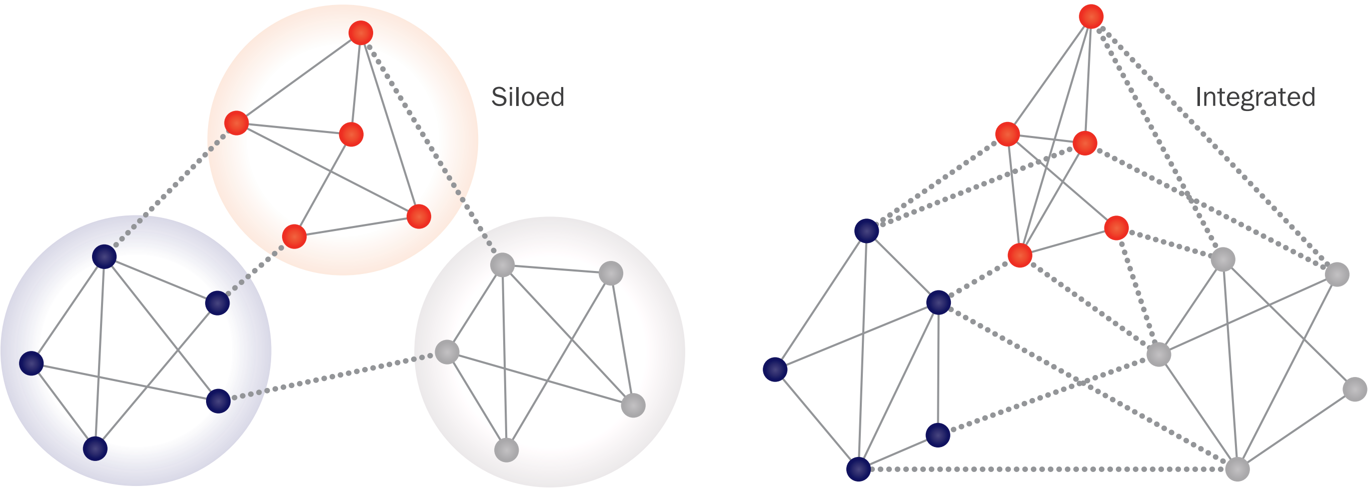
Relational integration seeks to determine if relationships are siloed or integrated across important boundaries within the network. As illustrated in Exhibit 4, integrated organizations or individuals easily share information and resources because the boundary does not influence the extent to which network partners are able to engage in relationships with one another. Within a siloed network, information is mainly shared within and not across a given boundary. In other words, the boundary represents a barrier that hinders relationships and information sharing across the entire network. Examples of boundaries that may hinder relational integration include geographic location, jurisdiction, function, type of organization or unit, or formal roles.

Siloed networks risk slow or non-existent information and/or resource flow across important boundaries in the network. In addition, the network may be less able to adapt quickly to both internal and external changes. For example, if a change is made within one boundary of the network, this update may not reverberate out to other groups in the network due to constrained information flow between silos. Finally, the ability of groups within the network to receive new or updated information from partners outside of their own boundary is lessened. Consequently, while a good amount of information may be flowing within a silo, information may still not provide all the necessary data, news, or intelligence important for the function of all the groups within the network.

Relationship Role Redundancy

An analysis of role redundancy seeks to assess the extent to which individuals or organizations are similar based on their relations to others in the network (i.e., have redundant ties). This may also be thought of as relational or structural "equivalence.” Identifying redundancy is based on calculating the similarity or dissimilarity of nodes, and then searching for patterns and simplifications. Redundancy is quantified by calculating the percentage of overlap between two

Exhibit 4 | Siloed Versus Integrated Communication Networks



Source: Booz Allen Hamilton

organizations or individuals of interest. Examining whether redundancy builds resilience (essential) or blocks efficiency (non-essential) can be illuminated by the qualitative assessment of organizational roles, responsibilities, and the like.

An analysis of the extent to which there is role redundancy between key nodes in the network helps to identify network risks as well as where there is flexibility and "backup" coverage. In general, when nodes have similar roles or formal obligations to interact with other partners in a network, some redundancy between particular organizations would be expected and beneficial. A moderate amount of overlap indicates that if one organization fails to pass on information or resources to others in the network, they have coverage from other partners to ensure that important information is disseminated throughout the system. However, if the networks of two organizations are highly redundant, then the partners are not providing any unique information or resources to others in the network. Consequently, a lack of any overlap or a complete overlap is a risk to network information dissemination and efficiency.

Providing ONA for DHS and Emergency Management Partners

Utilizing ONA, Booz Allen helped the Transportation Security Administration (TSA) Intermodal Security Training and Exercise Program (I-STEP) in its role in evaluating homeland security core capabilities such as Intelligence & Information Sharing capabilities for the Transportation Systems Sector. Through an I-STEP seminar and workshop, this initiative focused on the state of Nevada's transportation security information sharing and intelligence among stakeholders at the private sector, Federal, State, and local levels. TSA representatives included federal security directors from Las Vegas and Reno, the Transportation Security Operations Center, and the Federal Air Marshals Service. The planning committee recognized that transportation security partners in Nevada utilized multiple sets of plans and procedures for intelligence information sharing and wanted to gain a common understanding of information flow in both routine and crisis scenarios. For the first time, ONA was used to analyze and portray communications networks across the state.

During the November 2011 seminar, Federal, State, and local agencies presented their information-sharing processes and capabilities to approximately 80 participants. During the event, an information-sharing environment survey was distributed to collect communications information in three situations: (1) routine or day to day; (2) a top-down (federal to state and local) intelligence flow; and (3) a bottom-up (local to state and federal) intelligence flow. Subsequently, in a January 2012 workshop, participants reviewed the ONA findings and evaluated next steps to increase the effectiveness and resiliency of their transportation security networks.

Among the key findings was the need to focus on routine communications and increase the size of the state's communications networks. In addition, the ONA findings highlighted the importance of some key organizations as brokers of information, which connect a broader range of organizations across the network, as well as identified email procedures to ensure consistent communications linkages between organizations by combining discussion-based exercises and ONA in light of continual personnel changes among transportation security partners over time. This initiative is the first to utilize ONA as a tool to examine information-sharing networks among transportation security partners at the federal, state, and local levels. The seminar/workshop's success highlights the pivotal role that exercises combined with ONA can bring to industry and transportation security partners across the country.

Conclusion

ONA can empower stakeholders with the knowledge to be able to make decisions related to communications and collaboration on both a routine exercise and non-routine basis. As a proven methodology, ONA reveals the characteristics, composition, and structure of existing networks to help stakeholders gain unique insights into how organizations share and process information. Applied to federal, state, local and private security partners, exercises combined with ONA is a powerful tool that will enable leaders to design and build efficient whole community networks that foster resiliency and preparedness.

Booz | Allen | Hamilton

About the Authors

Christopher P. Bell is a lead associate at Booz Allen Hamilton where he provides homeland security, emergency management, and humanitarian assistance project management and consulting services to a variety of clients including the Transportation Security Administration, Federal Emergency Management Agency, Defense Department, and the United States Agency for International Development. His background includes project management, exercise design and development, facilitation, program evaluation, and training. He is a Certified Emergency Manager, Project Management Professional, and Master Exercise Professional. He graduated from Augustana College with a Bachelor's degree in Geography and DePaul University with a Master of Science degree in International Public Service Management.

Elizabeth Conjar is an associate at Booz Allen Hamilton where she provides survey research and organizational network analysis (ONA) services to a variety of clients including the Transportation Security Agency (TSA), Defense Intelligence Agency (DIA), NASA, and the International Finance Corporation (IFC). Her background includes experience in organizational and program assessment; quantitative and qualitative research and analyses; and social science methodology development. She is currently completing her doctorate in Industrial/Organizational Psychology at George Mason University.

Contact Information:

Christopher P. Bell
Lead Associate
bell_christopher_p@bah.com
703-412-7741

Elizabeth Conjar
Associate
conjar_elizabeth@bah.com
703-377-4858

About Booz Allen

Booz Allen Hamilton has been at the forefront of strategy and technology consulting for 100 years. Today, Booz Allen is a leading provider of management consulting, technology, and engineering services to the US government in defense, intelligence, and civil markets, and to major corporations, institutions, and not-for-profit organizations. In the commercial sector, the firm focuses on leveraging its existing expertise for clients in the financial services, healthcare, and energy markets, and to international clients primarily in the Middle East. Booz Allen offers clients deep functional knowledge spanning consulting, analytics, mission operations, technology, and engineering—which it combines with specialized expertise in clients' mission and domain areas to help solve their toughest problems.

The firm's management consulting heritage is the basis for its unique collaborative culture and operating model, enabling Booz Allen to anticipate needs and opportunities, rapidly deploy talent and resources, and deliver enduring results. By combining a consultant's problem-solving orientation with deep technical knowledge and strong execution, Booz Allen helps clients achieve success in their most critical missions—as evidenced by the firm's many client relationships that span decades. Booz Allen helps shape thinking and prepare for future developments in areas of national importance, including cybersecurity, homeland security, healthcare, and information technology.

Booz Allen is headquartered in McLean, Virginia, employs more than 23,000 people, and had revenue of $5.76 billion for the 12 months ended March 31, 2013. For over a decade, Booz Allen's high standing as a business and an employer has been recognized by dozens of organizations and publications, including *Fortune*, *Working Mother*, *G.I. Jobs*, and DiversityInc. In 2014, Booz Allen celebrates its 100th anniversary year. More information is available at www.boozallen.com. (NYSE: BAH)

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

Booz | Allen | Hamilton

Principal Offices

Huntsville, Alabama
Sierra Vista, Arizona
Los Angeles, California
San Diego, California
San Francisco, California
Colorado Springs, Colorado
Denver, Colorado
District of Columbia
Orlando, Florida
Pensacola, Florida
Sarasota, Florida
Tampa, Florida
Atlanta, Georgia
Honolulu, Hawaii
O’Fallon, Illinois
Indianapolis, Indiana
Leavenworth, Kansas
Aberdeen, Maryland
Annapolis Junction, Maryland
Hanover, Maryland
Lexington Park, Maryland
Linthicum, Maryland
Rockville, Maryland
Troy, Michigan
Kansas City, Missouri
Omaha, Nebraska
Red Bank, New Jersey
New York, New York
Rome, New York
Dayton, Ohio
Philadelphia, Pennsylvania
Charleston, South Carolina
Houston, Texas
San Antonio, Texas
Abu Dhabi, United Arab Emirates
Alexandria, Virginia
Arlington, Virginia
Chantilly, Virginia
Charlottesville, Virginia
Falls Church, Virginia
Herndon, Virginia
McLean, Virginia
Norfolk, Virginia
Stafford, Virginia
Seattle, Washington

The most complete, recent list of offices and their addresses and telephone numbers can be found on www.boozallen.com