

White Paper

Privacy and Security Best Practices for Use of At- Home Agents in a Federal Contact Center

Information Security and Privacy
Shared Interest Group
Work-At-Home Policy Task Force

Date Released: January 22, 2010

The Federal Government is under pressure from citizens to provide quick, accurate, and timely support. In many instances, this support is best administered using a temporary or geographically dispersed workforce. Additional pressure to integrate disabled veterans and other disadvantaged groups has resulted in changes in the way services are being delivered. This White Paper defines the “at-home agent” as an individual working for the Government or a contractor at his or her own home or other remote location. The benefits of the “at-home” workforce are summarized, followed by an investigation of the resistance that has been voiced against the use of such workers.

The IS&P SIG Work-At-Home Policy Task Force conducted an informal survey that was followed up by in-depth interviews to try to isolate the concerns and determine how Federal policy could be applied. Best practices from some successful programs are provided as guidelines on what has worked for others. Finally, a resource list is provided for managers who might want to take advantage of this valuable asset.

3040 Williams Drive, Suite 610, Fairfax, VA 22031

www.actgov.org • (p) (703) 208.4800 (f) • (703) 208.4805

American Council for Technology/Industry Advisory Council

The American Council for Technology (ACT) is a nonprofit educational organization, established in 1979 to assist the Government in acquiring and using information technology (IT) effectively. In 1989, ACT established the Industry Advisory Council (IAC) to bring industry and Government executives together to collaborate on IT issues of interest to the Government. In 1997, ACT established the Intergovernmental Advisory Board (IAB) to foster communication and collaboration between IT executives at all levels of Federal service—Federal, state, and local, and tribal governments.

ACT, in cooperation with IAC and IAB, is a unique, public-private partnership, dedicated to helping Government use technology to serve the public. The purposes of the organization are to communicate, educate, inform, and collaborate. ACT also works to promote the profession of public IT management. ACT and IAC offer a wide range of programs to accomplish these purposes.

ACT and IAC welcome the participation of all public and private organizations committed to improving the delivery of public services through effective and efficient use of IT. For membership and other information, visit the ACT-IAC Web site at www.actgov.org.

Information Security and Privacy Shared Interest Group (IS&P SIG)

The IS&P SIG is one of nine shared IAC interest groups. The IS&P SIG's mission is to help organizations incorporate security and privacy into their business processes to achieve compliance and mission success. The group meets monthly in the Washington, D.C. metropolitan area.

Disclaimer

This document has been prepared to provide information on a specific issue. It does not—nor is it intended to—take a position on any specific course of action or proposal. Nor does it endorse or recommend any specific technology, product, or vendor. The views expressed in this document do not necessarily represent the official views of the individuals and organizations who participated in its development. Every effort has been made to present accurate and reliable information. However, ACT-IAC assumes no responsibility for consequences resulting from use of the information herein.

Copyright

This document is copyrighted by the American Council for Technology in 2010. This document may be quoted, reproduced, and distributed without permission, provided that credit is given to the American Council for Technology and the Industry Advisory Council.

Further Information

For more information, contact the American Council for Technology and the Industry Advisory Council at (703) 208-4800 or www.actgov.org.

Overview

This White Paper investigates privacy and security policies that impact using at-home agents, provides a definition for at-home agents, and summarizes the trends that lead to the increased use of at-home agents. We also discuss managers' concerns that limit using at-home agents and identify best practices for evaluating whether the Government can use at-home agents and, if so, how best to implement policy to enhance their use. Input for this White Paper includes interviews with and commentary from Federal, non-profit and private sector participants in at-home agent issues.

Citizens now expect accurate, complete, and timely support any time of the day or night. As citizens expectations have changed, they have become more perceptive in using electronic access to services and more demanding in their expectations. Agencies have been compelled to implement multi-channel approaches to their citizen interactions, with traditional call centers augmented by Web-based and mobile solutions. However, it is not possible to provide full support simply by providing a Web site, even one backed up with a strong knowledge management system. Many citizen inquiries and requests still require human intervention to fully understand and respond to the request. Thus, the call center, staffed with live agency personnel, continues as a vital part of citizen/Government interaction. At the same time, increased broadband accessibility, workforce flexibility, costs of maintaining call center facilities, and technology decentralization capabilities are causing federal agencies to focus on using at-home agents and teleworkers as part of their call center workforce.¹

The expertise to respond to customer contacts cannot always be provided from a central call center or physical location. The trend towards teleworking and alternative workplaces means that agencies must examine the use of at-home agents as an alternative to respond to their customer contacts. The private sector has a long history of using at-home agents and has successfully addressed the issues of privacy and security for handling financial, credit card, personal history, health care, and other sensitive transactions. The issue is not whether the technology exists to support at-home agents—we know that there are many technologies to enforce the policy.

Commercial organizations, such as Citigroup, Inc, Master Card, American Airlines, General Electric, Ticket Master, Home Shopping Network, AAA Auto Clubs, 1-800 Flowers, Alamo Car Rental, Jet Blue, Medco Health Solutions, Office Depot, American Express, AOL, LLBean, Hewlett Packard, Hertz, Staples, Global Hyatt, Marriott International, Fed Ex, Walgreens, McKesson Health Care, Verizon, JCrew, AIG, Proctor and Gamble, Blue Cross/ Blue Shield, Comcast, Direct TV, Best Buy, Delta Airlines, and Hilton Hotels were identified by the Task Force as having successfully embedded at-home agents as part of their customer support strategy. Federal contact centers have been slower to adopt at-home agent, primarily citing the security and privacy requirements that are specific to the Federal Government.

This White Paper summarizes the findings of the At-Home Policy Task Force, by providing best practices and references to documents, web sites, and other material relevant to the use of at-home agents in a Federal contact center. URLs for web sites and publications have been provided as footnotes so that the reader can access the most current version of documents. Copies of publications are available in the ACT-IAC Knowledge Bank for member access.

¹ This White Paper refers to the Federal agency workforce (including contractor personnel) providing these responses as “agents”

Table of Contents

American Council for Technology/Industry Advisory Council.....	2
Information Security and Privacy Shared Interest Group (IS&P SIG)	2
Disclaimer	2
Copyright	2
Further Information.....	2
Overview.....	3
I. Background.....	5
II. Definition of an At-Home Agent	6
III. Privacy and Security Issues With At-Home Agents	7
IV. Trends Leading to Using At-Home Agents	10
V. Concerns Regarding Use of At-Home Agents.....	12
VI. Existing Federal Government Security and Privacy Policies Applicable to At-Home Agents	13
VII. Methodology	15
VIII. Best Practices	17
IX. Information Sources.....	21
X. Acknowledgements.....	23

I. Background

The E-Government Act of 2002² recognized the need to change the way Federal agencies communicate with and deliver services to citizens, businesses, and other agencies. The Act changed the manner in which agencies interact with their constituents through the Internet and through agency sponsored contact centers. As a result, the Office of Citizen Services and Communications (OCS) within the General Services Administration (GSA) was created as the managing organization for this e-Gov initiative. In addition to the broad range of services provided by OCS (USA.Gov, Federal Citizen Information Center, and best practices, among others), OCS also sponsors the Government Contact Center Council (G3C)³, an organization of more than 50 Federal contact centers operated by 35 Federal agencies.

Recently GSA USA Services Federal Services Division identified six types of customer contacts with the Government:⁴

- Informational
- Beneficial
- Dutiful
- Commercial
- Intergovernmental
- Other

According to a GSA Report, *Government-Wide Assessment of Citizen Services Activities Final Report*, there are more than 6,500 citizen-facing activities, of which 2,843 are telephone and 597 are e-mail or Web forms that require agent response actions. Together, these two channels represent nearly 47 million contacts per month or more than 51% of total activity. The Report also states that more than 32,000 full time employees (FTEs) support these two activities. In another report, *Citizen Service-Level Expectations: Phase 2 Supplemental Study*, convenience is cited as the top expectation, followed by competent service. These findings lead to the conclusion that qualified contact center agents is a key to a successful Federal contact center. One of the major considerations with contact center agents, in an office or at home, is the citizen's information privacy and security, which this white paper addresses.

² www.egov.gov

³ <http://www.usaservices.gov/communities/CouncilofGovernmentContactCenterLeaders.php>

⁴ <http://www.usaservices.gov/aboutus/CustomSegmentation.doc>

II. Definition of an At-Home Agent

An at-home agent is a Government employee or contractor who supports contact center activities from his or her home. This service may be provided on a full-time (remote agent) or part-time (telework agent) basis. Other terms used for at-home agents include remote customer service representative (CSR), virtual CSR, and mobile CRS.

Characteristics shared by both remote and telework agents include:

- Receives telephone, e-mail, fax, chat, or new media (e.g., Web 2.0) inquiries from an agency customer, prepares the response, and manages the contact through successful resolution
- Contacts are routed to the agent based on pre-defined rules and availability of the agent through an agency-controlled call distribution system
- Workload varies daily, weekly, monthly, annually, and randomly
- Available to meet variations in workload
- Works out of his or her home—full or part time
- Equipment used includes Government-provided equipment, personal systems, or a mix of Government and personal equipment
- Geographic location of an agent in relation to the agency may make on-site inspections and in-person oversight difficult or expensive

Unique characteristics of telework and remote at-home agents include, but not limited to:

- ***Telework At-Home Agent***
 - Works out of both an agency provided office and the agent's home location
 - Number of days working at home varies based on situation
 - Agents are limited by geographic location near an agency office
- ***Remote At-Home Agent***
 - Works entirely out of home office
 - Not restricted to any geographic location

III. Privacy and Security Issues With At-Home Agents

The ACT-IAC Information Security and Privacy Shared Interest Group Task Force was established to address several specific concerns that have been expressed related to security and privacy in the use of at-home agents. Some of the concerns cited and addressed in this White Paper include:

- How do I incorporate at-home agent equipment and software into my security certification and accreditation (C&A) to maintain Federal Information Security Management Act (FISMA) compliance, including compliance with Federal Desktop Core Configuration (FDCC)? This is an especially big concern when the equipment is not Government issued.
- How do I develop a Privacy Impact Assessment (PIA) to address Personally Identifiable Information (PII) that might be handled by an at-home agent? Privacy concerns are the most common ones raised. Many contact centers fear that private information will be unintentionally (or intentionally) compromised if allowed to leave the physical contact center facility and/or Government provided, provisioned, and maintained equipment.
- What controls are necessary to protect information from unauthorized use by either the agent or others in the household? This concern is over access by persons who have not been checked out by the Government. Within a facility, control can be exerted over who has access. Within a home environment, it is difficult to control who has access to a computer or if others might be looking at the data on the screen.
- How do I maintain control of the agent's home environment, short of providing and maintaining a set of Government-provided equipment? This is primarily a budget concern over the cost of the equipment and the cost for its maintenance, since equipment must now be serviced at the employee's home.
- How do I secure equipment at the agent's home? The concern here is that any security must be remotely administered in an environment that cannot be controlled.
- Privacy and Security implementation is not consistent across agencies. Each agency, and in many cases offices within agencies, has a unique mission through which it implements security and privacy. Therefore, what “works” for one agency does not fit another agency's mission.

The Task Force identified some key best practices specific to security and privacy that lead to successful implementation of an at-home agent program. These include:

- **Address security and privacy early**—security and privacy are often used as barriers to implementing an at-home agent program. Start by assessing the data that the agent will be handling and the ability of your IT infrastructure to support secure communications with at-home agents. In the end, barring any classification issues, security and privacy can be assured through a combination of technology and personnel trust.
- **Work with IT to develop security measures:** Detailed consideration of the risks, and their management, of permitting at-home agents to use their own computers and other equipment vs. agency provided systems.
- **Evaluate data that the agent will handle** -- Prior to determining what, if any, at-home agent program can be implemented, it is essential that you categorize the data from a security and privacy perspective. This process includes consideration of:

- **Security categorization**—FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems, and NIST SP 800-60 Rev. 1, Guide for Mapping Types of Information and Information Systems to Security Categories: (2 Volumes).⁵ In particular, SP 800-60, Appendix C, contains a detailed list of data types, together with guidelines for classifying the data; and
- **Privacy**—Chapters 2 and 3 of NIST SP 800-122, *DRAFT Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*.⁶
- **Evaluate existing and required security and privacy controls**—all Federal IT systems must undergo a C&A, which includes a PIA, regardless of whether the agents work at the agency facility or at a home or remote office. Discuss the content of the C&A and what controls are in place to manage the risk. While it is simpler to control risk by controlling physical parameters of a work site, do not assume this is necessary; build your case for expanding the boundaries into home and remote offices.
 - **Assess System and Data Security Risk**—with the increase in telework, most agencies have policies for employees who must work at home. These policies should include whether the agent uses Government provided equipment or personal systems. They should also include policies for how the agent connects to the Internet and agency systems when working from home and what devices they are permitted to use. Many agencies have moved to a virtualized environment to keep private and sensitive information off an employee’s system. Understanding your agency’s security posture as it applies to the telework situation will enable you to determine better how to deploy at-home agents.
 - **Physical Security of the Home Office**—some contact center representatives we interviewed stated that their organization required at-home agencies to work out of separate rooms with a lock; others reported that they required only a dedicated work area. In all cases, however, it was made clear that working at home is not a solution for caring for children or the elderly. It was expected that the agent would have a babysitter or nurse as they would when they were in the home office/designated work area. An agency’s at-home agent agreement should make it clear what the expectations are and, should the agent have a situation that needs to be addressed, address it on an individual basis.
- **Personally Identifiable Information (PII)**—NIST SP 800-122, *DRAFT Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*⁷, provides great guidance and advice. Several key issues to address are:
 - What PII will be displayed to an agent?
 - Is the agent permitted to print or write down this information? Consider whether writing or printing will make the call progress better.
 - If information is written or printed, how is destroyed at the end of the call? Consider providing an approved shredder for your agent.

⁵ http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf and http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol2-Rev1.pdf

⁶ <http://csrc.nist.gov/publications/drafts/800-122/Draft-SP800-122.pdf>

⁷ <http://csrc.nist.gov/publications/drafts/800-122/Draft-SP800-122.pdf>

- Is any PII stored on the agent's computer? This will depend on the systems you are using. Many contact centers have implemented Citrix or similar systems that do not leave any data stored on the agent's computer.
- How long is PII permitted to remain in your contact center data bases? The Privacy Impact Assessment (PIA) should define these rules. Unless the data is required for long-term use, such as processing grant applications, it is recommended that PII be wiped 60-90 days after its last use.
- **Personnel Security**—trust is the key element for at-home agents. Even the best policies and procedures can be compromised when trust does not exist. Two best practices for assuring personnel trust are:
 - **Background Investigations and Homeland Security Presidential Directive (HSPD)-12**—also known as, Personal Identity Verification (PIV), the HSPD-12 process incorporates background investigations, collecting biometrics, and issuing chip-enabled identity cards to authenticate and authorize an agent. Although not in wide use outside the Department of Defense, these cards, which contain encryption keys, can be used to activate computer equipment. Check with your IT department on the supported capability. When outsourcing contact centers and permitting the contractor to use at-home agents, require the contractor to perform background checks on all their employees and to provide a plan for monitoring their at-home agents.
- **Mandatory training for security and privacy**—All agencies require mandatory security and privacy training. Satisfactory completion of this training should be documented in the agent's personnel record. This task force recommends that the standard agency security and privacy training be modified to include specific requirements and procedures for working at home. Include topics, such as:
 - Setting up the physical environment with security and privacy in mind
 - What is considered PII and how to protect it
 - How to destroy any PII that is written down
 - Procedures for reporting a potential breach (do not make this an ominous task or agents will not report)
 - How to manage other persons in the home during working hours
 - Restrictions on using Government-provided equipment and supplies

IV. Trends Leading to Using At-Home Agents

The primary benefits cited for using at-home agents are financial and performance. These benefits are supported by the results of Government and private sector studies on telework and work at home experiences. For example:

- **Increased Focus on Telework:** As a mechanism that improves work-life balance, increases retention, reduces environment pollutants, and reduces costs. The well-defined work activities and performance metrics associated with a contact center make it an excellent candidate for teleworking. The Office of Personnel Management (OPM) and the Government Services Administration (GSA) provide resources to establish a viable telework program.⁸
- **Critical Element of Continuity of Operations and Disaster Recovery Planning (COOP/DR):** The ability to work at home during a crisis, emergency, or disaster enables a contact center to be more responsive. During these times, workload may increase dramatically so that agents must work longer hours, facilities may be affected to the point that agents cannot come into a physical center, or work hours must be shifted. Citizens and other constituents expect responsive support, even more so during times of crisis. At-home agents are less affected by the need for a physical facility and can adapt more readily to the increased demands of a crisis or emergency.
- **Access to Disabled Veterans and Other Handicapped Persons:** The Federal Government has increased the pressure to provide employment to our returning disabled veterans, many of whom possess significant knowledge and the interpersonal skills essential for an effective contact center agent. Depending on the disability, working at home can play a major role in providing accommodations as required by the Americans with Disabilities Act (ADA)⁹. Further, many contracts require using AbilityOne¹⁰ resources. The AbilityOne program, formerly the Jacob-Wagner-O'Day (JWOD), was created by the Jacob-Wagner-O'Day Act, to leverage the Federal Government's buying power to provide jobs for persons with disabilities. The National Industries for the Severely Handicapped (NISH)¹¹ and the National Industries for the Blind (NIB)¹² provide resources and access to organizations that can support these initiatives.
- **Expand Employment in Economically Depressed Areas:** As part of the American Recovery and Reinvestment Act (ARRA), many Federal, state, and local government agencies have undertaken initiatives to provide employment opportunities to rural areas and areas hit by heavy unemployment. One of the largest barriers to using at-home agents in rural areas has been access to high-speed Internet. The Broadband USA initiative provides \$7.2 billion dollars to remove this barrier¹³.
- **Government "Brain Drain":** As senior employees are retiring, the Government is losing a valuable resource. Many of these employees are still willing to work, but want more flexibility, such as variable hours and working from retirement locations. An at-home agent

⁸ <http://www.telework.gov/>

⁹ <http://www.ada.gov/>

¹⁰ <http://www.abilityone.gov>

¹¹ <http://www.nish.org>

¹² <http://www.nib.org>

¹³ <http://www.broadbandusa.gov/>

program provides the flexibility for these persons to enjoy the life style they select and enables the Government to take advantage of their expertise.

A joint GSA/Telework Exchange report, *The Benefits of Telework*¹⁴, highlights many benefits of teleworking and at-home agents. According to the report, key benefits stemming from mainstream implementation of telework include:

- A workforce that is capable of teleworking on a regular basis is also capable of leveraging its decentralized work settings to maintain continuity of operations (COOP) in the face of a natural disaster, terrorist attack, or other emergency situation.
- Telework contributes to a greener environment by diminishing vehicle carbon emissions as a result of a truncated or nonexistent employee commute.
- Teleworkers' job performance has been documented to either exceed or remain on par with that of workers in a traditional workplace arrangement.
- Telework increases personal freedom and flexibility, thereby improving morale and decreasing stress.
- A strong telework program improves employee retention and recruitment by increasing an employer's attractiveness in the current competitive job market.
- Telework accommodates persons with disabilities.
- Telework permits more time for employees to care for their loved ones.
- Telework can enable reduced demand for office space as well as reduced facility operating costs.
- Telework allows for optimal use of technological advances.

The OPM published a 2009 annual report on the Status of Telework in the Federal Government. This report¹⁵ shows an increase in workers who work full or part time from their homes. Twenty-seven agencies reported benefits that included morale, productivity, performance, transportation, and human capital.

¹⁴ <http://www.teleworkexchange.com/pdfs/The-Benefits-of-Telework.pdf>

¹⁵ http://www.telework.gov/Reports_and_Studies/Annual_Reports/2009teleworkreport.pdf

V. Concerns Regarding Use of At-Home Agents

For a variety of reasons, the Federal Government has been reluctant to permit the use of at-home agents as part of Government agency contact centers. Some concerns, in addition to privacy and security cited in Section III, that the ACT-IAC Information Security and Privacy Shared Interest Group Task Force identified and addresses in this White Paper include:

- How do I determine whether my agents can work at home? Many managers would like to allow their agents to work at home, but do not know what boundaries might exist. It is sometimes easier to deny the request than to justify it without clear guidelines, using security and privacy as their denial's justification.
- How do I manage agents working at home where I cannot observe their behavior? This is a management training issue since many managers feel they cannot manage what they cannot see.

The 2009 Status of Telework in the Federal Government Report¹⁶ identified the following barriers to telework, as reported by the agencies:

- Office coverage
- Management resistance
- Organizational culture
- IT Security
- IT Funding

These concerns are real. However, solutions do exist to address each. Research of existing policies and literature, as well as discussions with existing contact centers and case studies presented at conferences, provide solutions that enable managers to move forward with confidence.

¹⁶ http://www.telework.gov/Reports_and_Studies/Annual_Reports/2009teleworkreport.pdf

VI. Existing Federal Government Security and Privacy Policies Applicable to At-Home Agents

The Task Force's first step was to research current federal policies that might apply to, security, privacy, and other issues related to using at-home agents. We identified a number of resources. Below is a quick reference to some of the more relevant existing policy and guidance:

National Institute of Standards and Technology (NIST)¹⁷. NIST participated in our interviews and identified several documents applicable to at-home agents, including its June 2009 report on *Security for Enterprise Telework and Remote Access Solutions*.¹⁸ This Report provided suggestions for securing the infrastructure and detailed existing NIST publications that provide guidance. The three primary resources recommended for Government at-home agent programs include:

- ***SP 800-46 Revision 1, June 2009, Guide to Enterprise Telework and Remote Access Security***,¹⁹ is recommended as the first source for guidance on setting up an environment for at-home agents. This SP provides recommendations, which are identified in Chapter VII, Findings, and Best Practices. NIST also identifies technologies that can fortify security and privacy. In addition to the technical recommendations, SP 800-46, Appendix C, incorporates an extensive list of resources for telework security. This Task Force recommends that the reader consult these resources for additional in-depth information.
- ***SP 800-122, January 2009, DRAFT Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)***,²⁰ provides guidance on identifying and protecting PII, which is a key reason cited by managers for not permitting call center agents to work at home. Key to the NIST recommendations is identifying and categorizing PII, which is essential if an organization is to protect the PII. Examples are provided, along with recommendations for protecting PII. In the event that a breach happens, the report recommends a process for responding to the incident. SP 800-12, Appendix H, provides an extensive list of additional resources.
- ***FIPS PUB 201-1, March 2006, Personal Identity Verification (PIV) of Federal Employees and Contractors***,²¹ addresses procedures for identity proofing, conducting background checks, and authenticating employees and contractors who have access to Federal resources. These procedures are essential to assure that at-home agents can be trusted to handle private information. As with the other NIST publications, FIPS Pub 201-1, Appendix G, provides an extensive list of additional references.

The OPM and GSA have developed *Telework.gov*²² to support agencies and employees in developing telework programs. This portal provides links to many resources, including policies and procedures.²³ The *Guide to Telework in the Federal Government*²⁴ provides a great primer for setting up a telework program, including guidance on policies and procedures. Likewise, *Key Practices for the*

¹⁷ <http://csrc.nist.gov/publications/>

¹⁸ <http://csrc.nist.gov/publications/nistbul/June2009-Telework.pdf>

¹⁹ <http://csrc.nist.gov/publications/nistpubs/800-46-rev1/sp800-46r1.pdf>

²⁰ <http://csrc.nist.gov/publications/drafts/800-122/Draft-SP800-122.pdf>

²¹ <http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf>

²² <http://www.telework.gov/>

²³ http://www.telework.gov/policies_and_procedures/index.aspx

²⁴ <http://www.opm.gov/pandemic/agency2a-guide.pdf>

*Implementation of Successful Telework Programs*²⁵ provides solid recommendations for establishing a program.

Non-Government resources also exist. Among these resources is Telework Exchange.²⁶ The Exchange “is a public-private partnership focused on demonstrating the tangible value of telework and serving the emerging educational and communication requirements of the Federal teleworker community.” Their Web site, www.TeleworkExchange.com, provides a wealth of resources for managers and employees. Telework Exchange’s newsletters and events, including the Town Hall Meetings, are heavily attended by Government and provide up-to-date information on teleworking in the Federal Government. Telework Exchange participated in this Task Force as both a member of the Task Force and as an interview participant for policies. Their Resource Center²⁷ provides links to many resources, including securing a telework environment.²⁸ Another Non-Government resource is the white papers released by, and programs developed by, ACT-IAC that frequently address security and privacy. For example, the IS&P SIG recently held a panel discussion with three of the interviewees for this White Paper to discuss how they have addressed their concerns over privacy and security. The presentations can be found in the Knowledge Bank on the ACT-IAC Web site²⁹.

Many private sector white papers should be considered by any organization seeking to implement or expand its use of at-home agents. These white papers are often from commercial sources and reference particular solutions. Examples of these commercial white papers include:

- DMG Consulting’s Call Center At-Home Agents Best Practices³⁰
- LiveOps’ *Best Practices for Recruiting and Managing Remote Agents with a Virtual Contact Center Model*³¹
- Ernst and Young’s Risk at Home: Privacy and Security Risk in Telecommuting Checklist³²

²⁵ http://www.telework.gov/tools_and_resources/key_practices/index.aspx

²⁶ <http://www.teleworkexchange.com/>

²⁷ <http://www.teleworkexchange.com/resource-center.asp>

²⁸ <http://www.teleworkexchange.com/resource-center-resources-security.asp>

²⁹ <http://www.actgov.org>

³⁰ <http://www.dmgconsult.com/publications/>

³¹ <http://www.liveops.com/resource-library/index.html>

³² [http://www.ey.com/Publication/vwLUAssets/Risk_at_home -](http://www.ey.com/Publication/vwLUAssets/Risk_at_home_-_)

[Privacy and security risk in telecommuting checklist/\\$FILE/Risk%20at%20home_checklist.pdf](http://www.ey.com/Publication/vwLUAssets/Risk_at_home_-_Privacy_and_security_risk_in_telecommuting_checklist/$FILE/Risk%20at%20home_checklist.pdf)

VII. Methodology

The Task Force's proposal to research and report on the Federal Government's at-home agent policies was approved by the IS&P SIG Government Advisory Panel (GAP) in August 2008. The Task Force's objectives included:

- Identifying real and perceived problems
- Analyzing existing policy and guidelines and their application
- Developing a resource list for persons interested in further information
- Summarizing recommendations for using at-home agents within current privacy and security framework

Two deliverables were planned: a panel discussion that was held in September 2009 and this white paper. Members of the Task Force included volunteers from the SIG's membership, as well as representatives from the National Industries for the Severely Handicapped (NISH) and Telework Exchange.

To accomplish our objective, the Task Force adopted the following methodology:

- **General Survey**— the Task Force developed a survey using Survey Monkey. This Web-based survey was focused on getting information on general trends and perceptions. The survey was announced through the Government Customer Support Newsletter (a Government-sponsored newsletter that is published monthly on-line for contract center managers and staff). Due to the timing of the survey's release (December 2008–January 2009), the response was low and did not provide much of the information we sought.
- **Case Studies**—to counter the low survey response, we conducted case studies to understand who was using at-home agents and understand their level of success.
- **Individual Interviews**—from the case studies, the Task Force developed two interview formats: one for policy makers, the other for contact center operations. We then proceeded to conduct in-depth surveys (approximately 45 minutes) with the following:
 - Cindy Auten, Telework Exchange
 - Jim Ball, Alpine Access Consulting
 - John Connolly, InspiriTec (a NISH Affiliate)
 - Bo Hofstead, Goodwill Industries of North Florida (a NISH Affiliate)
 - Patrick Howard, Nuclear Regulatory Commission (NRC)
 - Michael Longwell, Working Solutions
 - Mark Middendorp and Peggy Gritt, National Industries for the Severely Handicapped (NISH)
 - Karen Scarfone, National Institute for Science and Technology (NIST)
 - Corina Stretch and Lauri Lehman, Puget Sound Energy (PSE)
 - MJ Willard, National Telecommuting Institute (a NISH Affiliate), who support the IRS contact center with at-home agents
 - Elliott Williams, Dell
- **Panel Discussion**— from the interviewees, the Task Force selected three persons to participate in a panel discussion. The three individuals selected were:
 - Cindy Auten, Telework Exchange, provided an overview of policies and what Federal agencies were doing to increase using telework and at-home agents

- Corina Stretch, PSE, described their program that allows agents to work at home up to four days per week. She described the lessons learned from their pilot program and how PSE planned to move forward to increase participation in the program.
- Michael Longwell, Working Solutions, described how they manage 76,000 at-home agents who work full-time from their homes with their own equipment. He described their security and privacy controls that are tailored to each customer's needs.
- **White Paper**—this White Paper summarizes the resources identified by the task force and best practices that were distilled from the research and interviews.

VIII. Best Practices

When this project was initially conceived, the Task Force focused primarily on agents working at home full time using their own equipment. During the interview process, we discovered that this is only one model. Other models are categorized as follows:

- **Telework Agent**—this is an agent who has a home office from which he/she works several days a week (the amount of at-home time varies depending on the situation). This model requires that the agent live within commuting distance of the office and have the ability to come into the office at regular intervals. A telework situation works well as a reward system for better performing agents and is ideal for preparing for COOP/DR situations. Contact centers that have implemented this arrangement seem pleased and have been expanding the number of agents in their telework program. The most common equipment setup for telework agents was for the agency to provide them with the equipment (usually a laptop for mobility and a printer in their home) which the agency can control.
- **Remote Agent**—a remote agent is one who works solely from a home office and, in many cases, uses their personal computers. This approach allows for a more global reach for the best talent and supports rural employment programs of the current Administration. While the model poses some issues, such as recruiting and training personnel remotely and using personal equipment, these problems have been successfully addressed by a number of contact centers.

Best Practices—regardless of the model selected, several best practices stood out:

- **Obtain management buy-in**—all successful at-home agent programs have management buy-in. This requires the contact center managers to prepare a case to demonstrate the benefits of the program and clearly state how they will monitor its success. The most significant impediment to management buy-in was the resistance by middle managers to allow agents to work from home. Many managers want to see their staff to “know they are working.”
- **Leverage your Agency’s telework policy**—Every agency – even those that do not actively deploy at-home agents – has a telework policy and a telework coordinator. The at-home agent is simply another form of telework and any implementation of an at-home agent program should be compliant with an agency’s existing telework guidelines.
- **Conduct pilot programs**—take baby steps when executing an at-home agent program. Our interviews showed that starting with a pilot program increased the success of using at-home agents. Pilot programs allow the contact center to refine its program incrementally. For example, what is the impact of the additional remote users on the IT systems? Pilots should last around six months and multiple pilots with expanding participation can be a sound approach to deploying the program.
- **Get a signed agreement with the agent**—this is a best practice for any telework program. The agreement sets forth the expectations and rules for working at-home. For example, one of our interviewees stated that they have a policy that, if the agent’s home system is down more than two hours, the agent must come into the office until his/her system is back up and running. The agency telework coordinator can help craft the initial agreement, which should be refined as part of the pilot programs.
- **Implement trial periods**—not all agents make good at-home workers. A consensus exists that a 90-day trial period for an individual is reasonable. Such a trial period allows time for the agent to settle in and for supervisors and managers to assess the agent’s performance.

During the trial period, it should be possible to identify problems with home networks, the home environment, or the inability of the agent to adapt to a home work situation.

Other Best Practices—have been distilled from our review of literature, case studies, and interviews include.

- Planning to use at-home agents
 - **Visit the Federal telework (Telework.gov) and Telework Exchange (TeleworkExchange.com) sites** to get a general roadmap for deploying an at-home agent program. Both these sites provide a wealth of resources for establishing your program. One step to consider prior to embarking on the program is to talk with your agency's telework coordinator: Every agency has a telework coordinator who has been trained on both Federal Government and agency-specific policies, procedures and mandates. Additionally, it is important to get a signed agreement between the agent and the agency/organization. This agreement should be renewed at least annually or when any modifications are made. At a minimum, this agreement should document job responsibilities, performance expectations, applicable policies and procedures, and reporting.
- **Managing at-home agents:** Several specific recommendations for managing at-home agents include:
 - **Document job responsibilities, requirements, procedures, and performance expectation** in the At-Home Agent Agreements.
 - **Conduct daily communications between supervisor and the at-home agent** to keep the agent connected to his/her supervisor. These communications can be as simple as a start-of-day e-mail or could include scheduled or unscheduled phone calls or chat sessions.
 - **Establish channels (e.g., chat) for at-home agents to collaborate with peers and supervisors.** Some form of instant communications (such as chat) is recommended so an agent can interact with his/her supervisor and other agents. This allows an agent to request support on a difficult calls and helps build a sense of community among the agents and supervisors.
 - **Hold team meetings on regular basis, preferably weekly,** including short team meetings. Proven technologies such as conference calls or a Web-enabled meeting enhance the sense of community. These meetings offer an opportunity for the agency to provide new information to the agents and allows agents a chance to communicate to both agency managers and other at-home agents on problems they encountered and/or solutions they developed.
 - **Develop a rewards program to incentivize at-home agents** because, as with any contact center, rewarding outstanding performance is a morale builder. Rewards do not necessarily need to be cash, but could include gift certificates to movies, restaurants, or some event, or even some paid time off. Consider what is important to the agent and try to develop rewards that encourage the agent's performance.
 - **Conduct audits** that can be in-person or virtual (using a Web camera installed on the agent's computer). The low cost of Web cameras enables visual communications with agents, which serves to improve the rapport between supervisors and agents, as well as serving as a tool for verifying the home setup.

- **Train managers and supervisors** on tools and techniques for managing at-home agents. This training will help break down the barriers and provide supervisors and managers with the skills they need.
- **Training and coaching** at-home agents was cited as a key element in assuring security and privacy, as well as performance. Several recommendations include.
 - **On-line training program**—while it may be feasible to perform on-site training for agents in telework mode, it is expensive to bring agents working remotely into an office for training. Agencies can conduct initial training as part of the on-boarding process, but additional training is best delivered on-line. Such training might include:
 - Skill building courses taken during slack time
 - Remedial training identified by supervisors or quality assurance
 - Advancement courses that allow agents to learn new systems and grow according to a career plan
 - Knowledge learning that provides additional or new information to agents that they need to conduct their jobs.
 - Security and privacy training conducted at least annually
 - **Certification**—a formalized certification program is highly recommended for initial training and ongoing skills training. Such a program provides a visible growth path for the agent and provides a tool for routing inquiries. Start a new agent off with general inquiries and monitor the agent’s performance. Agents who demonstrate a good writing ability might be certified to handle e-mail inquiries. Agents who effectively handle irate callers could be certified to take these calls. As agents prove their capabilities, they can be certified for more difficult calls, with commensurate compensation.
 - **Incorporate real-time coaching and monitoring tools**—if not already incorporated in the contact center, consider real-time monitoring tools that allow coaching via the telephone. Such tools are readily available and provide supervisors the capability of assessing their staff in actual working conditions. Look for monitoring tools with exception alerts that would allow the supervisor to understand the agent presence and alert supervisors of long breaks or long calls.
 - **Allow time in the schedule for coaching sessions between agents and their supervisor**—schedule time for supervisors to speak with their agents on a one-to-one basis. Use recorded calls and other observations to provide constructive feedback to the agent. Encourage the agent to grow and take additional training. Such actions will improve agent retention.
- **Quality Assurance:**—the same quality assurance practices that make a good contact center apply whether agents work in the center or at home. Some specific recommendations to consider include:
 - **Implement an automated call recording tool**—it is not necessary to record all calls, although this is a possibility and could be useful. However, random call recording (more frequent for new agents), as well as flagged calls should be recorded.
 - **Score and calibrate results**—score and calibrate recorded calls against performance metrics and call quality. Use the feedback to determine where additional training is required and whether any changes are required to call handling procedures.

- **Use scoring as a tool to improve agent’s performance, not to punish them**—use scoring to identify areas where an agent can improve his/her performance. Do not use it as a mechanism for punishing or berating an agent. Positive reinforcement will improve the agent’s performance.
- **Provide mechanism for agent to flag a potential quality issue for follow up with supervisor or QA staff**—good agents know when they need help. Even when they complete a call, they may feel it was not well handled. Provide a mechanism to allow an agent to flag or call for a supervisor or QA review and get feedback.

On a final note—this Task Force recommends that clearer guidelines be provided either as part of the Federal Government’s Telework Program or from the White House to encourage the use of at-home agents. As with other telework programs, agencies should be required to explain why at-home agents are not viable for a given contact center. To accompany this guidance, better training to program level management is recommended to build the skills to support a home-based workforce.

IX. Information Sources

This section of the white paper was prepared to provide a compact source for relevant organizations and other information sources that we found helpful. Many of the references were used in the paper, but there are other useful sources that were not part of our study.

1. Government Organizations

- a. Telework.gov (<http://www.telework.gov>) is the official Federal Government telework Web site. It is maintained by the Office of Personnel Management (OPM) and General Services Administration (GSA). This site provides information on setting up a telework program, including policies and procedures. It also provides access to many documents and reports that can help a contact center manager establish an at-home agent program.
- b. National Institute of Standards and Technology (NIST) Computer Security Resource Center (CSRC) (<http://csrc.nist.gov>) maintains a series of publications that includes Federal Information Processing Standards (FIPS), Special Publications (SP), NIST Interagency Reports (IR), and Information Technology Lab (ITL) Security Bulletins. The more relevant publications have been referenced in this white paper, but many more are available, as well as updates to exiting reports, on the NIST CSRC Web site.
- c. Department of Defense (DOD) Civilian Personnel Management Service (CPMS) (<http://www.cpms.osd.mil/telework.aspx>) supports DOD's telework program and can provide additional guidance for managers within DOD to comply with additional DOD security and privacy policy.
- d. GSA provides Section 508 compliance guidance (<http://www.section508.gov>). Compliance with Section 508 accessibility for the handicapped is required under Federal law. In particular, the information provided by GSA will assist a contact center manager set up a home office for persons with handicaps.
- e. DOD's Computer/Electronic Accommodations Program (CAP) (http://www.tricare.mil/CAP/Initiatives/DOD_Education_Activity.cfm) elaborates on DOD's policy regarding accommodations for the handicapped, providing specific guidance based on DOD policy.

2. Non-Government Organizations

- a. Telework Exchange (<http://www.teleworkexchange.com/>) is a public-private partnership focused on demonstrating the tangible value of telework and serving the emerging educational and communication requirements of the Federal teleworker community. The organization facilitates communication among Federal teleworkers, telework managers, and IT professionals. Their Web site contains up-to-date information on telework, including many reports, tools, and links to resources.
- b. The Telework Coalition (<http://www.telcoa.org/>) is a non-profit membership organization dedicated to enabling virtual, mobile, and distributed work through education, technology, and legislation. Their Web site includes links to resources, including a section dedicated to virtual call centers.
- c. National Industries for the Severely Handicapped (NISH) (<http://www.nish.org/>) is a national nonprofit agency whose mission is to create employment opportunities for people with severe

- disabilities by securing Federal contracts through the AbilityOne Program . The NISH has more than 1,300 nonprofit affiliates (NPA). The NISH established a teleservices organization to support call center services for its member agencies. Their expertise on employing the handicapped persons, both at-home and in the office, should prove a valuable resource for contact center managers.
- d. National Industries for the Blind (NIB) (<http://www.nib.org/>) is similar to NISH, except that NIB works with the blind under the AbilityOne program.
 - e. National Telecommuting Institute, Inc, (NTI) (www.nticentral.org) is a non-profit disability organization that employs 650 home-based individuals with disabilities to handle Internal Revenue Service, Department of Labor, Veterans Administration work, as well as calls for private sector companies.

In addition to the organizations listed above, there are many white paper and conferences that address at-home agents. References to the most relevant material was provided in the footnotes throughout this white paper. Since new documents are continually being published and old documents updated or deleted it is not practical to attempt to provide a complete list in this white paper. We do suggest, however, that anyone interested in at-home agents monitor the Web sites provided in this section and look at the references in the footnotes, as many of them contain long lists of sources for additional information.

X. Acknowledgements

This ACT-IAC paper was researched and written by members of the Information Security and Privacy Shared Interest Group **At-Home Agent Policy Task Force**. Task Force members include:

- Mark Samblanet, Chair, Active Network
- John Aldridge, Focus Technologies
- Ron Ashby, National Industries for the Blind (NIB)
- Cindy Auten, Telework Exchange
- John Booze, Dell
- Jerry Byers, TechTeam
- Amy Fadida, A.M. Fadida Consulting
- Peggy Gritt, National Industries for the Severely Handicapped (NISH)
- John Huggins, TechTeam
- Mike Kutchever, MACK Consulting
- Mark Middendorp, NISH
- Robert Moody, TechTeam
- Meghan O'Neil, Telework Exchange
- Ken Salzman, CLMS
- Patricia Titus, Unisys

Special thanks goes out to the Government and industry participants in our surveys and panel discussion:

- Cindy Auten, Telework Exchange
- Jim Ball, Alpine Access Consulting
- John Connolly, InspiriTec (a NISH Affiliate)
- Bo Hofstead, Goodwill Industries of North Florida (a NISH Affiliate)
- Patrick Howard, Nuclear Regulatory Commission (NRC)
- Michael Longwell, Working Solutions
- Mark Middendorp and Peggy Gritt, NISH
- Karen Scarfone, National Institute for Science and Technology (NIST)
- Corina Stretch and Lauri Lehman, Puget Sound Energy (PSE)
- MJ Willard, National Telecommuting Institute (a NISH Affiliate)
- Elliott Williams, Dell

Finally, but not least, our thanks to the following ACT-IAC staff members who supported the Task Force throughout our long effort:

- Glenda Henning, Senior Director of Membership, Marketing and Operations
- John Shaw, Senior Manager, Shared Interest Groups

And to Tom Evans (KMK Consulting), Chair of the Information Security and Privacy (IS&P) Shared Interest Group (SIG) for his guidance and support.

For additional information, visit the IAC Web site at <http://www.actgov.org>.