ALTERNATE WORK SITES

Preserving Vital Functions

Before Disaster Strikes

Advanced Management Program

15 March 2002

Bill Baker
Robin Boyette
Chris Buzzard
Robin Gallant
Kash Grimes
Jerry Johnson
Rick Washinger

"Robin's Nest"

I. **PROBLEM**: The after-effect of the terrorist attacks of 11 September 2001 brought into stark reality the need to preserve vital functions for all levels of the Department of Defense (DoD).

The DoD maintains a highly concentrated workforce in various bases and offices across the nation and overseas. Had the "9/11" attacks succeeded in destroying more of the Pentagon or any building that hosts vital DoD functions, our ability to prosecute a war would have been severely degraded while vital functions were reconstituted.

Even under current heightened conditions, is the DoD as effective as it could be in protecting its vital functions at all echelons? The answer is…… NO!

II. **PROPOSAL**: Use alternate work sites to protect vital functions before a disaster strikes.

Hours after the "9/11" attack, President Bush activated the Continuity of Operations Plan (COOP) to prevent the collapse of essential government functions.[1] This plan began as a temporary measure but is now a permanent precaution, albeit somewhat scaled down. The DoD has some redundant centers of communication, command and control such as U.S. Space Command headquarters, but many DoD activities do not have plans to preserve vital functions in case of disaster.

This proposal is not a "one size fits all" plan. DoD activities must determine which functions should be preserved and decide if alternate work sites provide an effective and efficient means to protect those functions.

[1] Gellman, Barton and Schmidt Susan, "Shadow Government Is At Work In Secret", Washington Post, Mar 02

III. <u>ALTERNATE WORK SITES</u>. The logic behind using alternate work sites as a method of protecting vital functions is as simple as it is old…. "don't put all your eggs in one basket", at least not at one time. With appropriate planning and investment in Information Technology (IT), a localized disaster will not shut down, even temporarily, the vital functions of DoD activities.

For the purposes of this proposal, alternate work sites are not permanent work locations for employees; they are locations to be used on a regularly scheduled basis….i.e., once or twice a week.

Three types of alternate work sites are examined that would provide an effective means to protect vital functions prior to a disaster. These are: 1) Telecommuting from home; 2) Telecommuting from Regional Telework Centers; and 3) Satellite Offices. Additionally, staggered work hours/shift work is explored as an alternative for activities that cannot accommodate the alternate work sites proposal. Activities have the option of applying one or any combination of these alternatives.

A. <u>Telecommuting from Home</u>. This type of work site provides an effective location to perform designated functions during peak productive hours at a time when the majority of the workforce is centrally located.

1. Strengths.

a. Dispersion. Telecommuting from home provides the widest possible dispersion of vital functions by placing employees in the greatest number of disparate locations. Businesses such as Freddie Mac and other companies directly

affected in the "9/11" attack are viewing telecommuting as a very viable option in order to "decentralize intellectual property."[2] Telecommuting "provides greater assurances that entire enterprises will not be wiped out, makes multiple backups to remote sites somewhat simpler, and serves to reduce gasoline consumption as well as other environmental amenities."[3] Simply put, telecommuting "makes good business sense."[4]

b. Productivity. Research in the private sector shows that productivity increases by about 15%, generating significant savings for their companies. Sixty-nine per cent of telecommuters at AT&T stated they were more productive. (See Appendix A). IBM and other major corporations report similar experiences and note that distractions and interruptions frequently found in the office environment are eliminated.

2. Weaknesses.

a. Resources. The cost of funding additional computer hard-ware and software , equipment installation fees, licensing fees, and phone service required to conduct daily business present a significant funding issue. These costs are mitigated through by a regional equipment reallocation program and by employees using their own equipment and Internet Service Provider (ISP). When employees use their own equipment, the Government can provide an external/removable hard drive to store

[2] "Attacks Spark Interest in Telecommuting", Amy Joyce, Washington POST, 31 Dec 01, http://washingtonpost.com
[3] "A different View of Security- Time for Some Serious Rethinking", Linux Planet, Dennis E. Powell, http://www.linuxplanet.com/linuxplanet/opinions/3784/
[4] "Attacks Spark Interest in Telecommuting", Amy Joyce, Washington POST, 31 Dec 01, http://washingtonpost.com

unclassified information with a locking file cabinet to store the drive when the employee is not at home.

b. Security. An April 2001 survey by the Office of Personnel Management found many activities were concerned about telecommuting's impact on security, especially when the function requires access to highly classified or sensitive data. The concerns centered on the potential that unauthorized persons could gain access to classified files or systems within firewalls. Given current security concerns and technological constraints, we do not recommend performing functions requiring access to classified information in this environment. Other alternate work sites are more suitable to mitigate this weakness. However, more sensitive functions can be safely dispersed using telecommuting as security technology advances to encompass biometric recognition, virtual private networks and encryption software.

c. Reduced Management Control. Many managers prefer face-to-face communications fear lines of communication will be sacrificed when an employee is working off-site. There is anxiety about measuring and maintaining successful employee performance as well as concerns about allegations of disparate treatment from employees denied the opportunity to telework.[5] However, supervision under any system, including telecommuting, requires establishment of clear guidelines and unambiguous communication.[6] Managers must communicate and document the goals and expectations up-front and how employees will be evaluated on these goals.

[5] OPM Document "The Status of Telework in the Federal Government" 2001
[6] "Good Communication Key in Strong Telecommuting", David Shwartz, 21 July 2000, http://www.bizjournals.com/phoenix/stories/2000/07/24/focus2.html

Managers must understand that this requires a change of management style to results oriented management rather than "over the shoulder" supervision. Through development of a better planning process, an organization can actually improve the control and productivity of the activity. [A set of guidelines to assist managers in implementing a successful telecommuting program is provided in Appendix B.]

B. <u>Telecommuting from Telework Centers</u>. This type of work site requires employees to commute to a GSA contracted "shared" office environment on a prearranged availability schedule. These offices are fully supported facilities with on-site technical support, IT equipment and software, and coordinated connectivity to the employer's work site.

1. Strengths.

a. Dispersion. This work site arrangement provides greater dispersion of vital functions than where the employees report and perform those functions in a central office everyday. There are fifteen centers in the Washington D.C. metropolitan area, each providing up to thirty workstations, private offices, meeting rooms, and copy/fax machines to mimic the home office setting.

b. Productivity. The Office of Personnel Management (OPM) has documented numerous testimonials from employees from a wide spectrum of Government agencies who work at the centers. The testimonials uniformly convey a professional office setting with superior and reliable IT equipment, excellent staff and lack of distractions. All these attributes, the employees say, are conducive to greater functional productivity.

c. Security. The Telework Centers offer fulltime magnetic keycard access with lockable file storage access for sensitive information. This overcomes the weakness of controlling sensitive data noted with home telecommuting. Organizations that require access to classified information will need to negotiate with GSA to provide space for a controlled access room(s) with Secret Internet Protocol Routing Network (SIPRNET) terminals. These terminals should exist without storage media drives so that employees could access classified information but not be able to download or store that information.

2. Weaknesses.

a. Resources. Although telecommuting is supported by Public Law, rental/ lease costs will remain a concern for activities using this alternative. Protecting vital functions justify the required resources to cover these costs.

b. Reduced Management Control. Telework Centers still place the function and employee out of sight of the manager. Although this alternative provides a more structured environment, managers must address the same concerns discussed in home telecommuting. Managerial oversight can be achieved by scheduling a supervisor to telecommute concurrent with personnel from other vital functions. [We respectfully refer managers to Appendix B for a method to deal with reduced control issues.]

C. <u>Satellite Offices</u>. A satellite office is a Government owned or leased facility controlled by the command for use on a daily basis to protect vital functions. Similar to TeleCenter employees, personnel would perform vital functions on a rotational basis.

Alternatively, personnel could be assigned permanently. These sites could also serve as alternate report sites in the event of a disaster at the primary base or office.

1. **Strengths.**

a. Security. Satellite offices can be more individually tailored to provide a level of security and functionality that would not exist at a TeleWork Center. Continuously manned sites might require additional security monitoring that could entail additional security personnel resources.

b. Reduced Management Control. The level and presence of management would be similar to that of the current workplace in this option.

2. Weaknesses.

a. Resources. This is potentially the most costly alternative because of infrastructure and equipment expenses as you duplicate the office setup at another site. A way to mitigate this, when possible, is to locate the office at a regional Government activity where space and support are already available. Properly structured, this could provide a low cost facility with high security while maintaining an alternate report site within a reasonable distance from the primary activity.

b. Dispersion. Of the three alternate work sites this offers the least dispersion of vital functions. However, it is located away from the home office and does provide a highly functional alternate place of work after a disaster.

D. Staggered Work Hours/Shift Work. This solution is offered as a viable alternative for activities that are not in a highly concentrated area or region and/or have high security concerns with classified information.

1. Strengths.

a. Security. This alternative provides the highest level of security for classified information and materials. It also provides the highest physical security for the facility.

b. Resources. This alternative would probably cost the least but costs associated for night differential for civilian employees and the addition of security personnel for after normal working hours could be considerable. Shift work might alleviate some of these costs.

c. Reduced Management Control. The "perceived" reduction of management control for employees not reporting at the same time as the manager could be mitigated if some supervisory control is in the office to monitor work effort.

3. Weaknesses.

a. Productivity. The previously mentioned studies suggest that productivity is greatest telecommuting and away from office distractions. Distractions might be reduced under this alternative but would still exist.

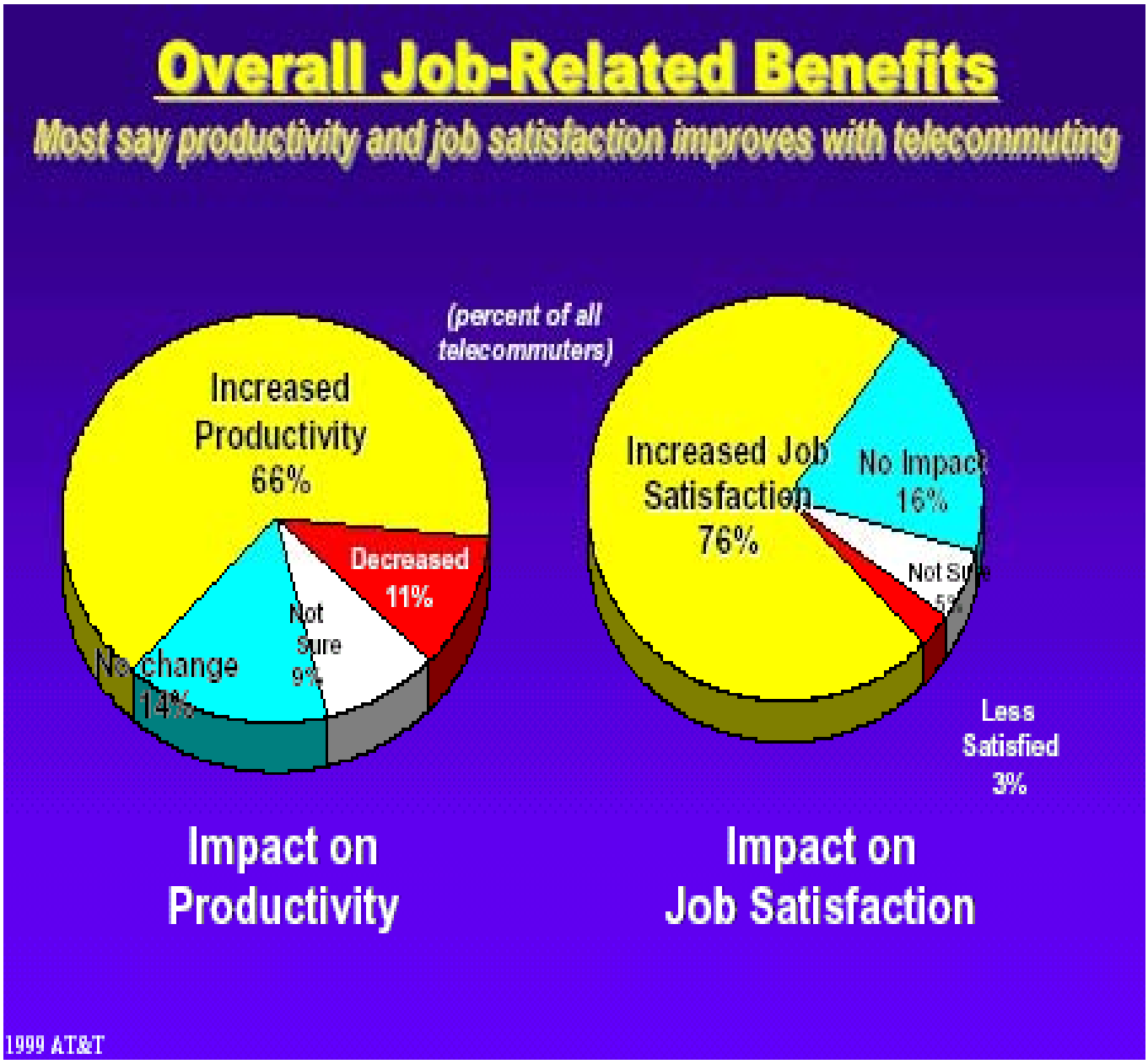
b. Dispersion. This alternative provides only time dispersion with no geographic dispersion and thus provides the least protection to vital functions.

IV. RECOMMENDATIONS. DoD's objective must be to preserve critical personnel, systems, and functions before a disaster occurs. Each DoD activity must identify their vital functions and prioritize them, investigate which one or combinations of proposed alternate work sites best fits their needs, and take action to provide the resources to make it happen. We strongly feel from our research that telecommuting is the best method to preserve vital functions in a disaster and deserves strong consideration

Although we did not discuss them in this paper our research revealed two concerns that any organization will need to consider. First, many data centers are physically co-located in high concentration along with other DoD activities. This presents a data protection issue just as important as protecting vital functions. We recommend, at a minimum, organization's vital data be backed-up at dispersed locations away from high concentration areas.

Finally, the basic elements of business case analysis will be required in any exhaustive study of this nature. We suggest that organizations address this. In their analysis, organizations might find that they can generate significant savings vice expenditures if they critically determine the vital functions that support their mission and carve out the rest.

APPENDIX A



http://wwwh.orc-dc.com/occupational/MeetingsArchive/2000/HighlightsAug2000/BlazekAug00.PDF

APPENDIX B

STEPS TO ACCOMPLISH IN BEGINNING A TELECOMMUTING PROGRAM

- **Determine Critical functions and essential personnel.**
- **Plan the program and determine the scope. Designate a coordinator.**
- **Identify the location (home, telecenters, libraries)**
- **Review DoD telework policy.**
- **Consider the following when selecting participants:**
  - ✓ **Does the employee have the attributes of a teleworker**
    - **Level of job knowledge/experience**
    - **Understand organizations objectives**
    - **Level of productivity**
    - **Quality of work**
    - **Results oriented**
    - **Adaptability of job to telecommuting**
    - **Organizational and planning skills**
    - **Project Management skills**
    - **Time management skills**
    - **Self-starter/motivator**
    - **Communication skills, both verbal and written**
    - **Technology literacy level**
    - **Productivity level with little to no supervision and feedback**
    - **Reliability and discipline at work**
    - **Flexibility to work in unfamiliar and changing situations**
    - **Desire and enthusiasm to telecommute**
- **Conduct good two way communication to foster trust and solicit employee input.**
- **Conduct training sessions for teleworkers and supervisors.**
- **Focus on results and how to measure.**
- **Monitor progress and maintain open and frequent communication.**

Steps obtained from AT&T "Getting Started" http://www.att.com/telework/get_started/

Authors:

CDR Bill Baker is Commanding Officer of the Priority Material Office, Bremerton,WA

Ms. Robin Boyette is Development Director at the Fitting Out and Supply Support Assistance Center, Norfolk, VA

Mr. Chris Buzzard is the Configuration and Logistics Information Manager at the Military Sealift Command, Washington, D.C.

Major Robin Gallant is Assistant Head of Accounting, Accounting Liaison Branch, Programs and Resources, Marine Corps Headquarters, Washington, D.C.

CDR(S) Kash Grimes is Director of the Critical Requirements Contracting Department at the Naval Inventory Control Point, Mechanicsburg, PA

CDR Jerry Johnson is Director of Production, Defense Distribution Depot, Norfolk, VA

Mr. Rick Washinger is Director, Program Management Division, Submarine Support Directorate, Naval Inventory Control Point, Mechanicsburg, PA