Office of Inspector General

December 2007
Report No. EVAL-08-002

The FDIC's Telework Program

Office of Evaluations

oig

Office of Evaluations

The FDIC's Telework Program

Background and Purpose of Evaluation

Since October 2000, the Congress has continued to express its desire for federal agencies to create viable telework programs through a number of legislative actions. Telework programs allow employees with appropriate work projects to work at home or in other approved work sites if they meet telework program requirements and obtain approval from their supervisors.

The Office of Personnel Management (OPM) and the General Services Administration (GSA) have joint leadership roles for the government-wide telework initiative. The two agencies provide services and resources to support and encourage telework, including issuing guidance to agencies in developing their programs and procedures. In doing so, the OPM has incorporated Federal Emergency Management Agency (FEMA) guidance for both continuity of operations and pandemic preparedness.

In May 2001, the FDIC introduced a Telework Pilot Program to give employees greater work/life flexibility while continuing to meet the Corporation's mission. The FDIC's telework program became permanent in May 2003.

Our evaluation objective was to assess the extent to which the Corporation has established and implemented a telework program that is consistent with applicable federal standards and guidelines and recognized best practices.

To view the full report, go to www.fdicig.gov/2008report.asp

Results of Evaluation

The FDIC has established a telework program that is consistent in most respects with applicable federal standards and guidelines and recognized best practices. In that regard, the FDIC's policies and program elements compare favorably to telework guidance of 13 other federal agencies we reviewed. In OPM's *2006 Federal Human Capital Survey*, FDIC employees reported an overall satisfaction rate of 56.6 percent with the Corporation's telework program compared to a rate of 21.8 percent government-wide.

Reported participation in FDIC's telework program grew from 20 percent in 2001 to 47 percent in 2006. In 2005, following a more restrictive definition of telework that defined qualifying frequencies, the OPM calculated the FDIC's participation level to be at 4.56 percent in its 2006 *Status of Telework in the Federal Government* report to the Congress. Further, the report showed that the FDIC's employee participation level ranked 59th among 77 federal agencies. The FDIC has its own views about gauging the success of its telework program, other than the level of participation, such as employees being able to utilize partial-day telework to attend appointments or other non-work events in order to achieve a better work/life balance. Other issues bring into question the reliability of the OPM statistics. For example, DOA noted that its time and attendance reporting system is not configured to capture the type of telework data that OPM requires and, as a result, the FDIC under-reported telework participation information to OPM. Accordingly, it is unclear whether the FDIC has sufficiently reliable data to draw valid conclusions regarding the extent of participation in its telework program. Finally, the FDIC could better assess its program by conducting an evaluation of the program, consistent with corporate policy, and establishing measurable goals.

The FDIC also needs to clarify the role that telework plays in its business continuity and pandemic event plans and policies, and conduct tests to evaluate the viability of telework arrangements under both scenarios. The FDIC reported to the OPM that the majority of FDIC employees are fully capable of sustaining operations while teleworking. However, the FDIC needs to do more to ensure that during an emergency, the Corporation would be fully functional within the time frames prescribed by FEMA, or should a pandemic event occur, the Corporation has the ability to maintain uninterrupted operations for an extended period.

The FDIC received an award in 2006 for its innovative use of technology to support employees who teleworked. Further, the Corporation has issued extensive guidance on protecting sensitive information and implemented controls to address OMB and GSA information security requirements associated with teleworking. Most notably, the FDIC requires two-factor authentication for user identification, and remote network sessions are encrypted. However, the FDIC needs to complete initiatives that will provide greater assurance that sensitive electronic information--stored on removable media and Personal Digital Assistant devices often used for teleworking--is safeguarded from unauthorized disclosure. The FDIC could also take steps to further protect data from unauthorized access during telework sessions on non-FDIC computers.

Finally, our report discusses two other matters for management's information and consideration—the FDIC's progress in developing and implementing a Pandemic Influenza Preparedness Plan and an opportunity for the FDIC to improve the efficiency of its administration of telework forms.

Recommendations: We made recommendations to improve the quality and reliability of telework participation data; conduct an evaluation to determine whether the FDIC's telework program is meeting management's expectations; ensure that teleworkers are prepared and supported during emergency situations and pandemic events; further enhance security over data used when teleworking; and improve the efficiency of telework forms. Management concurred or partially concurred with eight of our nine recommendations and offered a reasonable explanation for disagreeing with the remaining recommendation.

Table of Contents

ACRONYM LIST

AIS	Automated Information Systems
BCP	Business Continuity Plan
CBA	Collective Bargaining Agreement
COOP	Continuity of Operations
CU	Corporate University
DIR	Division of Insurance and Research
DIT	Division of Information Technology
DOA	Division of Administration
DOF	Division of Finance
DRR	Division of Resolutions and Receiverships
DSC	Division of Supervision and Consumer Protection
EEP	Enterprise Encryption Project
EIM	Enterprise Information Management
ERT	Emergency Response Team
FEMA	Federal Emergency Management Agency
FMR	Federal Management Regulations
FPC	Federal Preparedness Circular
GSA	General Services Administration
IT	Information Technology
NTEU	National Treasury Employees Union
OCFO	Office of Chief Financial Officer
ODEO	Office of Diversity and Economic Opportunity
OERM	Office of Enterprise Risk Management
OIA	Office of International Affairs
OIG	Office of Inspector General
OMB	Office of Management and Budget
OO	Office of the Ombudsman
OPA	Office of Public Affairs
OPM	Office of Personnel Management
PDA	Personal Digital Assistant
PIPP	Pandemic Influenza Preparedness Plan
RCN	Remote Computing Network
USB	Universal Serial Bus

Federal Deposit Insurance Corporation
3501 Fairfax Drive, Arlington, VA 22226

Office of Evaluations
Office of Inspector General

DATE: December 6, 2007

MEMORANDUM TO: Arleas Upton Kea
Director, Division of Administration

Michael E. Bartell
Chief Information Officer and Director,
Division of Information Technology

[Signed]
FROM: Stephen M. Beard
Assistant Inspector General for Evaluations and Management

SUBJECT: *The FDIC's Telework Program*
(Report No. EVAL-08-002)

This report presents the results of our subject evaluation. Telework, also referred to as telecommuting or flexiplace, has gained widespread attention over the past decade in both the public and private sectors as a human capital flexibility that offers a variety of potential benefits to employers, employees, and society. The term telework refers to work that is performed at an employee's home or at a work location other than a traditional office. Congress and the executive branch have shown interest in telework, primarily based upon the belief that its use will benefit the federal government. Benefits of telework include reducing traffic congestion and pollution, improving recruitment and retention of employees, increasing productivity, and reducing the need for office space. Employees also can realize benefits from teleworking, including reduced commuting time; lowered costs in areas such as transportation, parking, food, and wardrobe; removal of barriers for those with disabilities who want to be part of the workforce; and improvement in the quality of work life and morale accruing from the opportunity to better balance work and family demands.

EVALUATION OBJECTIVE AND APPROACH

Our objective was to assess the extent to which the Corporation has established and implemented a telework program that is consistent with applicable federal standards and guidelines and recognized best practices.

To accomplish our objective, we:

- Evaluated relevant FDIC policy and program elements against applicable government-wide guidance and recognized best practices,
- Interviewed program officials about the status of the telework program,
- Verified that the FDIC complied with the Office of Personnel Management (OPM) telework reporting requirements,
- Performed analysis of telework participation information to identify trends and usage among divisions and offices,
- Evaluated the efficiency of the FDIC's administration of the telework program, and
- Assessed the FDIC's guidance and efforts to ensure adequate security over information used by employees when teleworking.

We also engaged the accounting firm of KPMG, LLP (KPMG) to assess the FDIC's guidance and efforts to ensure adequate security over information that is processed, stored, and transmitted while teleworking. KPMG's engagement primarily involved:

- Evaluating the FDIC's four methods of remote access,
- Interviewing program officials about the status of initiatives intended to automate encryption of sensitive information stored on mobile computers and devices,
- Verifying that the time-out function for remote access methods functioned properly, and
- Assessing the FDIC's progress in logging data extractions and erasing them when no longer needed.

Appendix I describes in detail the objective, scope, and methodology of this evaluation.

BACKGROUND

Through a number of legislative actions, Congress has indicated its desire that federal agencies: create telework programs that establish program leadership; think broadly in setting eligibility requirements; allow employees, if eligible,[1] to participate in telework; and track and report telework program results. The most significant congressional action related to telework was the October 2000 enactment of Section 359 of Public Law No.106-346, which mandates that each executive branch agency establish a policy under which eligible employees may participate in telework to the maximum extent possible without diminishing employee performance. The legislation also requires agencies to designate telework coordinators who are responsible for overseeing the implementation of telework programs and serving as points of contact.

The legislative framework also assigns responsibility for leading the government-wide telework initiative to the OPM and the General Services Administration (GSA). Jointly, OPM and GSA manage a federal Web site[2] for telework, which is designed to provide access for employees, managers, and telework coordinators to a range of information related to telework, including

[1] An eligible employee is any satisfactorily performing employee of the agency whose job may typically be performed at least one day per week by teleworking.
[2] The joint Web site can be found at www.telework.gov.

announcements, guides, laws, and available training. OPM has primarily provided expertise in human resources issues and, in that regard, published *A Guide to Telework in the Federal Government*, dated August 2006, to guide implementation of the program. OPM has also determined that telework is an essential element in continuity of operations and pandemic[3] preparedness and incorporated Federal Emergency Management Agency (FEMA) guidance into its guide. GSA has generally addressed technical, equipment, and telework center issues and issued Federal Management Regulations (FMR) Bulletin 2007-B1 entitled, *Information Technology and Telecommunication Guidelines for Federal Telework and Other Alternative Workplace Arrangement Programs,* dated March 2007.

With regard to technical issues, the Office of Management and Budget (OMB) issued Memorandum M-06-16, dated June 23, 2006, to the heads of federal departments and agencies entitled, *Protection of Sensitive Agency Information*. OMB issued the memorandum in response to several data security breaches. The memorandum recommends that the departments and agencies implement a series of controls for safeguarding the remote access, transport, and storage of sensitive information. Effective implementation of these controls becomes particularly important to ensuring adequate information security as the Congress encourages greater participation in telework programs.

Consistent with its legislative mandate to track and report on the status of telework programs, the OPM requests telework data from all federal agencies by way of an Annual Telework Survey. Jointly, OPM and GSA use the information to provide a yearly snapshot of the federal government telework initiative that is published in an annual report to the Congress entitled, *The Status of Telework in the Federal Government* (Annual Telework Status Report).

In its *A Guide to Telework in the Federal Government*, OPM defined telework as any arrangement in which an employee regularly performs officially assigned duties at home or at another work site geographically convenient to the residence of the employee. In 2005, OPM and GSA established a more restrictive definition of telework that defined qualifying frequencies of at least 3 days a week, 1-2 days a week, or at least once per month. Previously, even if an employee teleworked less than once a month, the employee was included in the number of teleworkers reported to Congress. The 2005 Annual Telework Status Report indicated that 1.3 million of the 1.8 million federal employees in 78 Federal agencies were eligible to telework. Of the 1.3 million eligible employees, 119,248 or 9.51 percent, employees actually teleworked.

In May 2001, the FDIC introduced a Telework Pilot Program to give employees greater work/life flexibility while continuing to meet the Corporation's mission. In May 2003, the Corporation established a permanent program that allows for participation based on the specific nature and content of the work to be performed rather than on position, grade, or work schedule.

FDIC Circular 2121.1, dated May 16, 2003, entitled, *FDIC Telework Program*, provides the policy, program guidelines, general provisions, and responsibilities associated with the telework program. The FDIC's WorkLife Program Manager, who is part of the Division of

[3] Pandemic influenza is a global outbreak of disease that occurs when a new influenza virus appears or "emerges" in the human population, causes serious illness, and spreads easily from person to person worldwide.

Administration's (DOA) Human Resources Branch, is designated as the Telework Coordinator and is responsible for providing management advisory services related to the telework program.

EVALUATION RESULTS

The FDIC has established a telework program that offers a means of supporting the Corporation's goal of enhanced employee flexibility and improved work/life balance, provided that the efficiency of the FDIC and its mission are not adversely impacted. The FDIC's program is generally consistent with OPM's *A Guide to Telework in the Federal Government* as it relates to:

- Appointing a telework coordinator;
- Establishing telework policy, including determining eligibility, delineating responsibilities of managers and employees, creating and managing signed telework agreements, documenting denials, and applying uniform performance practices;
- Establishing policies on information systems and technology security;
- Establishing guidelines for equipment and support to be provided to teleworkers; and
- Providing, to a limited extent, telework training.

Further, in 2003, the FDIC established the Examiner's Option program wherein eligible examiners are permitted to work out of their homes or at approved alternative work sites when not working at an insured depository institution or at another required site. Under this program, the FDIC provides the employee with a one-time maximum reimbursement of up to $500 for costs associated with equipment not otherwise provided by the Corporation, and an annual reimbursement of up to $480 for costs associated with multiple telephone lines and/or high speed data transmission access.

In the 2006 *Federal Human Capital Survey*, conducted by OPM, FDIC employees reported an overall satisfaction rate with the Corporation's telework program of 56.6 percent compared to 21.8 percent government-wide.

Finally, in 2006, the FDIC received an award from the Telework Exchange, a public-private partnership focused on eliminating telework gridlock, for the Corporation's innovative use of technology to support employees who teleworked. The award was based primarily on the fact that the FDIC provides a variety of remote access services to support its telecommuting and mobile users and an access control method that enables virtually every eligible FDIC employee with access to a computer to participate in the FDIC's telework program.

EMPLOYEE PARTICIPATION IN THE FDIC'S TELEWORK PROGRAM

In 2004, the FDIC reported that 43.1 percent of its employees had teleworked. However, in 2005, following the establishment of a more restrictive definition of telework, OPM calculated the FDIC's participation at 4.56 percent in its Annual Telework Status Report.[4] For 2006, based on the statistics submitted to the OPM, we calculated an increase in participation to 5.16 percent. According to OPM's 2007 Annual Telework Status Report, the FDIC's participation level ranks relatively low among other federal agencies. Specifically, we compared the FDIC's standing with 77 other federal agencies that reported telework participation to OPM in 2005. Our analysis showed that the FDIC's participation level of 4.56 percent was among the bottom 25 percent of those agencies.

We also analyzed the impact that the more restrictive definition had on other agencies. We determined that 46 of the 67 agencies that reported telework statistics in both 2004 and 2005 had decreases in telework participation while the remaining 21 had increased participation. For agencies with employee populations under 20,000, the change in reported participation ranged from an increase of 3.42 percent at the Department of Housing and Urban Development to a decrease of 54.4 percent at OPM.

FDIC Employees Participating in Telework

We conducted analyses to gain additional insights into the extent of employee participation in the FDIC's telework program. For example, using the statistics that the FDIC provided to OPM, we determined that 47 percent of all FDIC employees participated in telework to some degree in 2006 and that the extent of participation varied by grade-level categories. (See Table 1 on the next page.)

[4] Recognizing the impact the new definition would have on the government's telework statistics, in its 2006 Report to the Congress, the OPM cautioned that comparison to past years' data is not meaningful. The new definitions have narrowed the definition of "teleworker," requiring a reasonable frequency of teleworking more in line with programmatic needs. The OPM further noted that the definition change contributed to the government-wide decrease in the number of teleworkers reported from 140,694 in 2004 to 119,248 in 2005.

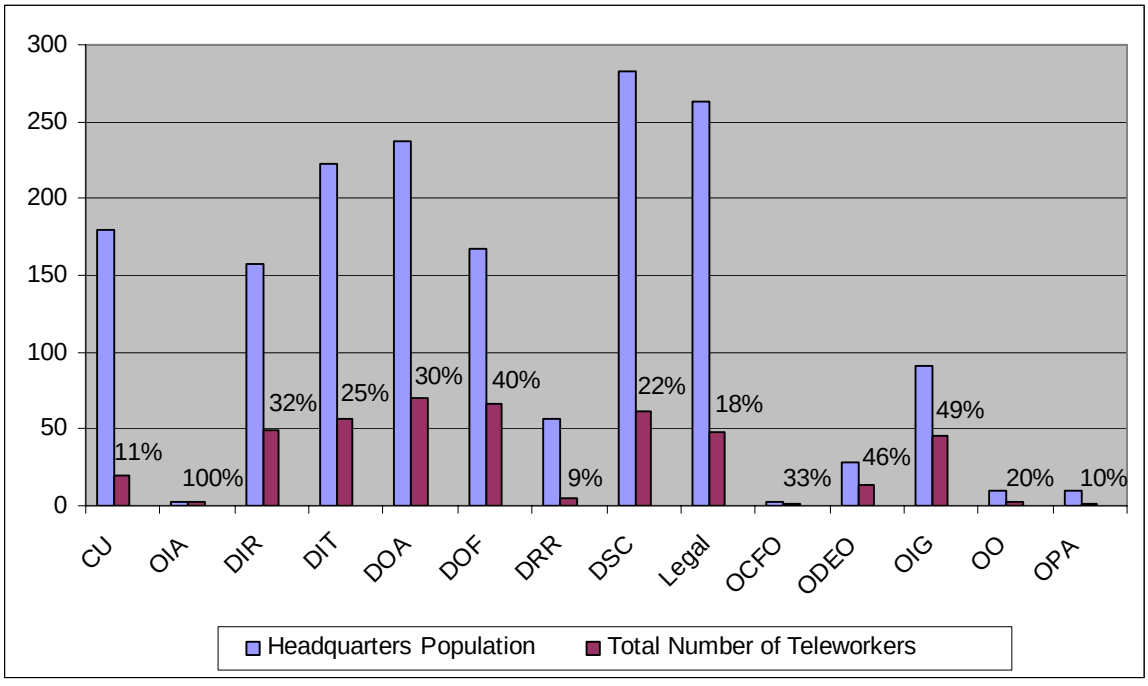
Table 1: 2006 Corporation-Wide Participation in the FDIC's Telework Program by Grade

Employee Grade Level	FDIC Employees	Teleworkers Report in OPM Survey*	Percent of FDIC Employees Participating
1 through 4	84	3	3.57%
5 through 12	2,158	1,035	47.96%
13 through 15	1,745	878	50.32%
CM-1 through 2	486	206	42.39%
EM	93	24	25.81%
Totals	4,566	2,146	47.00%

Source: OIG Analysis of the FDIC's Response to OPM's 2006 Annual Survey and DOA Demographics Statistics.
*The accuracy of the time reported in the CHRIS T&A System assumes that those who teleworked accurately coded their time as "telework" during each pay period.

We also determined that, based on the source data provided to OPM, 440 of 1,747, or 25 percent, of all eligible headquarters employees participated in the telework program in 2006. Figure 1 below provides a breakdown of the participation by headquarters activity.

Figure 1: 2006 Headquarters Participation in the Telework Program



Source: OIG Analysis of 2006 Telework Statistics provided by DOA. OERM participation was not addressed in the statistics.

DOA noted that beyond the OPM participation level criteria, DOA also has its own views about the success of its telework program, such as employees being able to practice partial day telework to attend medical appointments or other non-work events in order to achieve a better work life balance. While such telework events may not meet the OPM criteria, DOA believes they are important in gauging the success of the Corporation's telework program.

Reliability of the Telework Statistics

Several issues bring into question the reliability of the telework statistics that were reported to OPM, and the FDIC's participation levels and ranking must be viewed in the context of these issues.

- When OPM redefined telework in 2005, OPM was not clear regarding what constituted a "day" of teleworking. According to OPM, neither OPM nor anyone else has defined what constitutes a "day" of telework and OPM has received questions on the definition from various agency representatives. As a result, agency reporting of telework participation is likely to be inconsistent.

- When the FDIC provided telework statistics to OPM in 2005 and 2006 regarding the number of employees who teleworked on a regular, recurring basis, the Corporation only included examiners who were participating in the previously discussed Examiner Option program as teleworkers. The Corporation did so because it determined that these examiners best fit OPM's new telework definition and because CHRIS T&A was not configured to capture the type of telework data that OPM requires. DOA representatives stated that as a result, FDIC under-represented telework participation levels to OPM.

- The FDIC relies on the CHRIS T&A system to determine telework participation. Employees must select one of the 12 "telework" transaction codes when coding their time and attendance in order to be counted as teleworking. The FDIC lacks assurance that employees are coding their time and attendance in such a manner; thus, the Corporation may be underreporting the number of employees actually teleworking.

Conclusion

At first glance, the FDIC's reported levels of participation should be of concern to management as the Corporation should be following the lead of the Congress and Executive Branch in promoting and increasing telework in the federal government. Further, the FDIC may be missing opportunities to improve the quality of work life and morale of its employees. However, it is unclear whether the Corporation has sufficiently reliable data to draw valid conclusions regarding the extent to which employees are participating in its telework program. Statistics submitted are being included in a statutorily-required report to the Congress and do get attention from its members, other federal agencies, and the public.

Recommendation

We recommend that the Director, Division of Administration:

1. Take steps to improve the quality and reliability of data collected for the purposes of determining the extent of telework participation by FDIC employees.

EVALUATION OF THE TELEWORK PROGRAM

The FDIC could do more to evaluate the success and status of its telework program to ensure the program is meeting management's expectations. In this regard, neither the WorkLife Program Manager nor any of the nine divisions and offices we included in our review has conducted an evaluation of the telework program.[5] Instead, the FDIC has principally relied on time charges in the FDIC's time and attendance system as a gauge of the telework program's success. Prior to OPM's 2005 revised definition of telework, the FDIC's statistics showed the number of employees teleworking was approaching 50 percent. This figure was based on any time charged as telework by an employee in the CHRIS T&A system regardless of the number of hours worked. With such a high percentage of participation, management apparently determined there was not a need to perform a program evaluation.

Circular 2121.1, Section 10, *Evaluation,* states that to adequately assess the impact and success of the telework program, both employees and managers or supervisors are expected to participate in the evaluation. The evaluation may include the collection of both quantitative and qualitative data (including participation rates, office space needs, and other issues impacted by program use) requiring the completion of surveys or responses to interview questions. The Circular does not clearly address who should lead or conduct the evaluations or the required frequency.

DOA officials advised us that they were not aware of an overall evaluation of the program since it became permanent in 2003. Further, none of the nine divisions and offices we included in our review has conducted evaluations of their administration of the telework program. Division of Insurance and Research officials told us although they have not performed a formal evaluation, their senior management periodically discusses the division's stance on telework, how it is administered, and the fairness of its application. Division of Finance (DOF) management indicated they are working with representatives from DOA to gather statistics on DOF's participation in the telework program and to conduct a survey of their employees.

Finally, the FDIC has not established measurable telework program goals. Such goals can be used in conducting program evaluations for telework in such areas as productivity, operating costs, employee morale, recruitment, and retention.

Without a comprehensive program evaluation and measurable goals, it is difficult to assess whether the Corporation's telework participation meets management's expectations and is

[5] The nine divisions and offices included the Office of Enterprise Risk Management (OERM), Corporate University (CU), Division of Insurance and Research (DIR), Division of Information Technology (DIT), DOA, Division of Finance (DOF), Division of Resolutions and Receiverships (DRR), Division of Supervision and Consumer Protection (DSC), and the Legal Division.

reasonable considering the various factors that can impact the extent of telework at the FDIC. In conducting such an evaluation, the FDIC should address the following areas.

Leadership Attention

On June 12, 2007, the Government Accountability Office testified before the *Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia, Committee on Homeland Security and Governmental Affairs, U.S. Senate*, (*GAO-07-1002T)*, that the Telework Enhancement Act of 2007, S.1000, recognizes the importance of leadership in promoting an agency's telework program by requiring the appointment of a senior-level management official to perform several functions to promote and enhance telework opportunities. There is no consensus at this time regarding the specific duties of such an individual in relation to the duties of the agency officials currently designated as telework coordinators.

At the FDIC, oversight of the telework program has been made a part of the duties assigned to the WorkLife Program Manager. The WorkLife Program Manager also has responsibility for providing management advisory services relating to alternative work schedules, leave, dependent care, employee assistance, and other programs. In addition, the WorkLife Program Manager could be assigned to assist in issues related to classification and compensation, staffing and placement, and human resources development. The FDIC's approach to leadership of the program —a mid-level manager devoted part-time—may fall short of what is being contemplated in the pending legislation discussed previously and may need to be revisited.

Publicity and Training

We met with the WorkLife Program Manager to gain an understanding of recent efforts to promote and provide training on the telework program. The following examples were provided:

- DOA presented a program on telework in October 2006,
- New employee and Corporate Employee Program orientations address telework,
- Presentations are made at DSC regional conferences and other division conferences, and
- Presentations at certain WorkLife Program seminars include telework information when appropriate.

OPM guidance, as well as telework literature and guidelines, states that informing employees and managers of the program and publicizing it are key telework practices for implementation of successful federal telework programs. Training and information on the following aspects of telework may be beneficial to FDIC employees:

- Types of assignments and circumstances that are suitable for teleworking,
- Coding of time and attendance data,
- The types of information that would be appropriate for teleworkers to be handling and how sensitive information should be protected when teleworking,
- Home safety and technology considerations, and
- The role that telework plays in continuity of operations (as discussed later in this report).

Conclusion

There is continuing Congressional interest to expand teleworking in the federal government, and the FDIC's policy encourages use of the telework program for those projects/duties that are well-suited for completion at an alternative work site. Therefore, the FDIC should assess whether its program and participation level meet corporate expectations and are reasonable considering the various factors that can impact the extent of telework at the FDIC.

Recommendation

We recommend that the Director, Division of Administration:

2. Conduct an evaluation consistent with Circular 2121.1 to determine whether the FDIC's telework program is meeting management's expectations and desired outcomes. The evaluation could address, among other things:

    - Whether goals and objectives exist against which the success and impact of the program can be measured,
    - Fairness and consistency across the Corporation in how managers are administering the program,
    - Sufficiency of leadership and management attention, and
    - Extent of promotion, publicity, and training.

INCORPORATING TELEWORK INTO BUSINESS CONTINUITY AND PANDEMIC PREPAREDNESS

Telework is a key component of being prepared for and continuing operations during emergency situations. The FDIC could more fully and expressly incorporate telework into its business continuity planning and pandemic preparedness efforts. Doing so would provide the FDIC with greater assurance that its employees and infrastructure can maintain uninterrupted operations or be fully functional within the time frames prescribed by FEMA in the event of an emergency or pandemic event.

Emergency Preparedness Guidance

The FEMA's Federal Preparedness Circular (FPC) 65, Section 9. *Planning Requirements for Viable Coop Capability*, revised as of June 15, 2004, is applicable to all Federal Executive Branch departments, agencies, and independent organizations. FPC 65 defines Continuity of Operations (COOP) planning as an effort to ensure that the capability exists to continue essential agency functions across a wide range of hazard emergencies. COOP capability is intended to be short-term; it must be functional within 12 hours and may last up to 30 days.

Section 9 further states that the COOP must include regularly scheduled testing, training, and exercising of agency personnel, equipment, systems, processes, and procedures used to support the agency during a COOP event. Section 10, *Elements of a Viable Coop Plan*, states that tests and exercises serve to assess, validate, or identify for a subsequent corrective action program,

specific aspects of COOP plans, policies, procedures, systems, and facilities used in response to an emergency situation. Training familiarizes COOP personnel with the procedures and tasks they must perform in executing COOP plans.

The OPM incorporates portions of FPC 65 guidance into its *A Guide to Telework in the Federal Government*, which states that telework should be part of all agency emergency planning and that management must be committed to implementing remote work arrangements as broadly as possible to take full advantage of the potential of telework to ensure that:

- Equipment, technology, and technical support have been tested.
- Employees are comfortable with technology and communications methods.
- Managers are comfortable managing a distributed workgroup.
- Expectations are communicated both to the Emergency Response Team (ERT) and non-ERT employees regarding what steps they need to take in case of an emergency.
- Business Continuity Plan (BCP) expectations are integrated into telework agreements as appropriate.
- Essential personnel who might telework in case of an emergency are allowed to telework regularly to ensure functionality.

The section of the OPM Guide entitled, *Practice, Practice, Practice*, states that the success of an organization's telework program depends on regular, routine use. Experience is the only way to enable managers, employees, IT support, and other stakeholders to work through any technology, equipment, communications, workflow, and associated issues that may inhibit the transparency of remote work. The OPM Guide concludes that individuals expected to telework in an emergency situation should, with some frequency, telework under non-emergency circumstances.

Business Continuity Plans, Pandemic Influenza Preparedness Plan, and Telework Agreements

The FDIC stated in its report to OPM in the *2006 Call for Telework Data* that telework has been fully integrated into its emergency preparedness/COOP plans. However, neither the Washington, D.C., area's 2006 BCP, dated January 2007, nor the divisional BCPs contain references to telework, although some divisions require their staff to remain at home during emergency situations. We discussed the need to incorporate telework in the BCPs with the FDIC's Assistant Director, Security Management Section. The Assistant Director agreed that telework is not specifically mentioned in the BCPs but stated that Corporation employees understand that telework will be the means they use to continue or resume operations.

With regard to pandemic preparedness, the Assistant Director confirmed that telework is the cornerstone of the FDIC's pandemic plan but added that there are many telework-related issues that must be addressed before the Pandemic Influenza Preparedness Plan (PIPP) is completed and implemented. We discuss the FDIC's progress in completing a pandemic preparedness plan later in this report under the section entitled, "Other Matters."

Finally, we noted that Form 2121/05, *Employee/Supervisor Telework Agreement*, does not specifically address the Corporation's expectation that telework will be a key component of employees continuing or resuming operations.

Training

As discussed earlier in our report, the FDIC's telework training has concentrated on the benefits derived from teleworking and has not addressed telework in the context of continuity of business operations. None of the training provides hands-on experience that ensures an employee is capable of teleworking from a remote site. Further, the FDIC's Corporate University (CU) does not offer technical telework training specifically designed for FDIC employees. DOA should coordinate with CU to ensure that telework training addresses the role that telework plays in maintaining continuity of operations as discussed in recommendation 2.

FDIC Employees Equipped to Telework

In 2005, the FDIC reported to the OPM that 3,784 of its 4,515 employees that were eligible to telework were equipped, trained, and ready to telework in the case of a long-term crisis.[6] In 2006, the FDIC reported that 4,570 employees were eligible and 4,435 were prepared to telework. These statistics represented all employees that had received a SafeWord® authenticator token. While the number of tokens issued was a valid indicator of the FDIC's progress toward preparing its employees to telework, it was not necessarily representative of the actual number of employees who successfully participated in the telework program.

On our behalf, DOA researched this issue and found that from July 1 through August 31, 2007, 3,414 unique user accounts, or 77 percent of all user accounts, were used to access the FDIC network through one or more of the remote access systems. By refining the list, the Division of Information Technology (DIT) determined that there were 822 headquarters accounts and 2,592 regional/field office accounts on the list of remote access users for this period. The high number of field accounts (86 percent of all field accounts) was expected because examiners generally use remote access methods to obtain access to the FDIC's network. With regard to the headquarters accounts, 822 accounts represent 53 percent of headquarters accounts.

Telework Tests

The FDIC's employees have not been required to practice telework under simulated emergency conditions. The Assistant Director, Security Management Section, confirmed that the FDIC has not conducted practice tests of the emergency operations. In October 2006, the FDIC sponsored a Corporate Telework Week. Employees were encouraged to telework, at a minimum, one day during that week. The number of teleworkers was measured through the FDIC Time and Attendance system. During this event 870 FDIC employees teleworked, making this period of participation the highest for all of 2006.

[6] In a subsequent section of this report, we discuss concerns with the training and readiness of employees for teleworking in a crisis.

According to KPMG, DIT has asserted that the FDIC has a fully redundant remote access solution that is able to support all FDIC employees. Specifically, DIT has deployed a Remote Computing Network (RCN) solution for its primary back-up site – the Richmond Data Center – with a software configuration that is nearly identical to the one used on a regular basis at Virginia Square. DIT also asserted that the Richmond Data Center RCN solution is capable of supporting 5,000 users. However, this assertion is based upon the technical designs of the RCN solution created during the 2003 or 2004 time frame. KPMG indicated that actual testing of 5,000 concurrent sessions should be conducted to ensure that the original RCN architecture remains capable of supporting such a large number of concurrent users with the addition of new applications and newer versions of Microsoft Office.

DIT acknowledged that the capacity of its remote access network had not been stress tested with remote workers but stated that in the event of a major business interruption that impacted multiple federal agencies, the true "Achilles heel" of agency business continuity planning would be the ability of the local telecommunications infrastructure to handle increased activity from thousands of remote workers. While this may be true, we believe there is merit in stress testing the FDIC's remote access network and verifying FDIC employees' technical ability to connect to the FDIC network remotely. Such a test could be as simple as requiring all, or a large number of, FDIC headquarters employees to work from home on a particular day and attempt to remotely log on to FDIC's network at a particular time.

Conclusion

The FDIC recognizes that telework is a key component to resuming or continuing operations in the event of an emergency or pandemic event and has taken some steps to ensure that its employees are sufficiently prepared and its technology solution is adequately designed to that end. However, consistent with OPM and FEMA guidance, the Corporation would benefit from taking further action to communicate and integrate telework into its business continuity and pandemic preparedness planning, ensure managers and employees are comfortable with telework arrangements, and validate that its technology solution works under simulated emergency circumstances.

Recommendations

We recommend the Director, Division of Administration:

3. Revise the FDIC BCPs and pandemic preparedness plans to more specifically describe the role telework plays in those plans.

4. Identify personnel who would be expected to telework during an emergency and include corporate expectations into their telework agreements.

5. Implement periodic testing of equipment, technology, and technical support associated with large numbers of employees concurrently teleworking in an emergency situation and require individuals expected to telework in an emergency situation to periodically telework under non-emergency circumstances.

SECURITY CONTROL REQUIREMENTS FOR TELEWORK

KPMG evaluated the security controls for telework and found that the FDIC has implemented a number of controls and has an on-going effort to fully address all of the security requirements of OMB Memorandum M-06-16, *Protection of Sensitive Agency Information*, dated June 23, 2006 (M-06-16). The FDIC has met the two-factor authentication requirement for user identification, and remote network sessions are encrypted. Also, the FDIC specifically addresses the telework program and provides guidance on protecting sensitive information when teleworking in its Annual Security Awareness Training that is required for all employees and contractors and has issued extensive guidance related to information security. However, work remains for the FDIC to complete its planned deployment of an enterprise-wide automated encryption solution for laptops, removable Universal Serial Bus (USB) devices, and Personal Digital Assistantws (PDA) to provide increased assurance that sensitive data stored on such equipment and devices will be appropriately protected. Further, the FDIC could take additional steps to protect data from unauthorized access during telework sessions on non-FDIC computers.

Methods for Teleworking

The FDIC provides four methods for remote users (e.g., teleworkers) to access the FDIC network. These services include Ascend Dial-In, RCN, FastAccess, and WebVPN.

> **Ascend dial-in** is available for use with FDIC laptops. The service provides dial-in access to the FDIC network using standard analog telephone lines to connect via a local access or national 800 number.
>
> **RCN** is a secure, Web-based remote access system available for use with home computers or FDIC laptops. Remote users access an FDIC secure gateway over the Internet, log in, and establish a remote session with an RCN server running a limited set of office applications.
>
> **FastAcess** is a Web-based remote access service intended to provide mobile users basic access to FDIC computing resources without having to install certificates or specialized software.
>
> **Web/VPN** is a secure remote access system intended to provide full network access to employees using FDIC laptops. A VPN is a network that can provide remote offices or individual users with secure access to an organization's network via the Internet.

Key Security Controls Associated with Teleworking

OMB Memorandum M-06-16 recommends the following security controls for safeguarding information removed from, or accessed from outside of agency locations: (1) encrypt all sensitive data on mobile computers and devices; (2) allow remote access only with two-factor authentication; (3) use a ‘‘time-out’’ function requiring user re-authentication after 30 minutes of inactivity for remote access and mobile devices; and (4) log all computer-readable data extracts

from databases holding sensitive information and verify that each such extract has been erased within ninety 90 days or that its use is still required.

Data Encryption

OMB M-06-16 recommends encryption of all data on mobile computers and devices that carry sensitive agency data. FDIC Circular 1360.9, *Protecting Sensitive Information*, dated April 30, 2007, requires that sensitive information stored on end-user IT equipment (e.g., laptop and desktop computers) as well as on removable media (e.g., diskettes, CD/DVD, USB flash drives, external removable hard drives) are to be encrypted. In addition, sensitive information should only be stored on corporate IT equipment. The current data encryption methods (Entrust, PKZIP, and Microsoft EFS[7]) are manual.

When employees telework and perform tasks using applications and data on the FDIC's laptops and network, the information is adequately protected regardless of which of the four available access methods they use—as long as the information remains within the network and is not downloaded to a home computer or storage device. In addition, the FDIC is working on an automated solution to ensure that sensitive information stored on mobile computers and devices is encrypted. In that regard, DIT initiated the Enterprise Encryption Project (EEP) in August 2006 with separate phases for encryption of laptops, removable media, and PDA devices. In our October 11, 2007 draft report, we reported that:

- The FDIC had selected Pointsec as the tool to encrypt data on laptops and as of September 20, 2007, DIT had installed encryption software on 2,500 of the approximately 3,800 agency laptops as part of Phase I of the EEP. The remaining laptops were scheduled to be encrypted as part of the Corporate Laptop Replacement Project by October 19, 2007.

- The FDIC was in the inception stage of Phase II of the EEP, the objective of which was to identify a software tool to encrypt removable storage devices that connect to a computer (such as USB drives). Phase II was scheduled to be implemented on January 25, 2008.

- Phase III of the EEP was scheduled to begin in January 2008 and entailed identifying an encryption solution for PDA devices. At the time of our draft report issuance, the completion date for Phase III had not been determined.

We concluded that manual data encryption methods could not ensure that all sensitive data stored on FDIC-provided mobile computers, storage devices, and PDAs was encrypted because these methods are prone to human errors and omissions. We reported that until the EEP is completed, sensitive data stored on FDIC IT equipment would be more vulnerable to unauthorized access if the media was lost or stolen.

DIT provided updated milestone information for the EEP project in November 2007. The FDIC completed Phase I encryption of all corporate laptops in November 2007. Regarding Phase II, encryption of removable media, DIT provided a project plan with detailed milestones which

[7] EFS only encrypts files stored on internal hard drives and cannot encrypt files stored on CD/DVD or USB storage devices. Users can encrypt files on DVDs and CDs using Entrust or PKZip

estimated completion of the encryption for USB drives in January 2008 and CDs by March 2008. Regarding Phase III encryption of PDA devices, DIT implemented a pilot in late November and anticipated full implementation of PDA encryption by the end of December 2007.

Two-Factor Authentication for Remote Access

OMB M-06-16 recommends that agencies allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access.

KPMG tested all four of the FDIC's remote access methods, Ascend Dial-in, RCN, FastAccess®, and WebVPN, and found that the four access methods meet the two-factor authentication requirement set forth in M-06-16. Remote access users are required to enter their network user identification and accompany it with their network password, a one-time key generated by a Safeword® authenticator token, and a 4-digit user-selected PIN before being granted access to the FDIC network.

Time-Out Function Requiring User Re-authentication After 30 Minutes of Inactivity

NIST Special Publication 800-53, Rev. 1, *Recommended Security Controls for Federal Information Systems* (NIST 800-53), requires that the information system automatically terminates a remote session after a maximum of 30 minutes of inactivity for remote access and portable solutions.

KPMG tested the time-out function for all four of the FDIC's remote access methods. The testing showed that the FDIC has instituted several functional time-out configurations for its four remote access methods that will automatically time out or disconnect the user after 30 minutes of inactivity. However, as shown in Table 2, several situations exist where remote connections are not successfully timed out after 30 minutes of inactivity as required by M-06-16.

Table 2: Time-out Function Test Results

Remote Access Solution	Remote Access Methods	Inactivity Time-Out (30 Minutes) Test		Max Session Time-Out (180 Minutes)Test	
		Outlook Closed	**Outlook Open**	**Outlook Closed**	**Outlook Open**
Ascend Dial-in	This method is available for use on FDIC laptops only.	Failed	Failed	Passed	Passed
RCN	RCN is intended for use with home computers or FDIC laptops.	Passed[a]	Passed[a]	Passed[a]	Passed[a]
FastAccess®	FastAccess® is intended for use with home computers or FDIC laptops.	Passed[a]	Failed[a]	Passed[a]	Passed[a]
WebVPN	WebVPN is available for use on FDIC laptops only.	Failed	Failed	Passed	Passed

Source: KPMG Evaluation Results. Test conducted from July 18 through 25, 2007.

Note: Access to the network through all remote access solutions is facilitated by the use of a Safeword® authenticator token (two-factor authentication). All four remote access solutions are configured to time out after 30 minutes of user inactivity or after 180 minutes regardless of activity.

[a] Same result when tested on personally-owned PC.

The FDIC is experiencing technical difficulties in implementing the 30 minute time-out configurations for Ascend Dial-in, FastAccess®, and WebVPN. Specifically, the network is not able to discern between actual user activity and background software services running on the computer such as antivirus and personal firewall computer processes.

Abandoned remote access connection sessions that do not properly time out after a period of user inactivity may be accessed by unauthorized users to gain access to sensitive agency data. As a compensating control, DIT has implemented a 15-minute password-protected screensaver on all FDIC computers. Testing revealed that FastAccess® failed to time out after 30 minutes of inactivity on a non-FDIC computer with an open session of Microsoft Outlook for e-mail service.

Logging Data Extracts and Erasing Extracts After 90 Days

OMB Memorandum M-06-16 recommends that agencies "log all computer-readable data extracts from databases holding sensitive information and verify each extract including sensitive data has been erased within 90 days or its use is still required." In addition, NIST 800-53 requires that organizations increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to organizational operations [or] organizational assets. Organizations are to employ automated mechanisms to integrate audit

monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.

The FDIC has not implemented a solution to automatically log all computer-readable data extracts from databases holding sensitive information and confirm its subsequent deletion within 90 days for data that is no longer needed. The FDIC is currently researching potential software solutions that will satisfy this M-06-16 requirement. Although DIT has initiated an effort to identify a data extract logging software solution that meets the technical and functional requirements for logging sensitive data extracts, DIT indicated that the commercial software market has not developed a suitable product to meet the FDIC's needs. DIT also indicated that this requirement is proving to be a challenge for most federal agencies.

With respect to extraction of sensitive data, if such activity is not logged, monitored, and its deletion confirmed after 90 days following its extraction, the extracted sensitive data could be vulnerable to unauthorized electronic copying and sending by individuals with malicious intent. In addition, RCN and FastAccess® could allow users to store sensitive information unencrypted on home computers that are vulnerable to unauthorized access.

Through discussions and limited testing, KPMG determined that as a compensating control, the FDIC's Enterprise Information Management (EIM) group is restricting the ability to copy production data to non-production environments by implementing a set of procedures for data requests. EIM has also published policy limiting access of production data for testing, quality control, and deployment preparation purposes to 45 days, at which point, access to the data is automatically removed.

Identifying Sensitive Information to be Used When Teleworking

In addition to KPMG's work on IT security, we determined that divisions and offices had not developed specific guidance identifying sensitive information related to their respective activities and operations that may not be appropriate for telework. Instead, the divisions and offices were relying on corporate-wide information security guidance. To better ensure that sensitive information is properly safeguarded when employees are teleworking, requests to telework should identify the data that will be used and its source, and that information should be considered in making decisions to approve or disapprove requests.

The FDIC has issued extensive guidance related to information security, for example:

- FDIC Circular 1300.4 – *Acceptable Use Policy for Information Technology Resources*
- FDIC Circular 1310.3 – *Technology Security Risk Management Program*
- FDIC Circular 1310.5 – *Encryption and Digital Signature for Electronic Mail*
- FDIC Circular 1360.1 – *Automated Information Systems (AIS) Security Policy*
- FDIC Circular 1360.9 – *Protecting Sensitive Information*

FDIC Form 2121/05, *Employee/Supervisor Telework Program Agreement*, states that applicable policies and directives related to equipment and information security, such as those mentioned above, apply to the telework program. Further, Form 2121/05 cautions that employees may be held responsible for security breaches or equipment damage due to negligence. Circular 2121.5,

FDIC Telework Program, Section 7. Paragraph d., states that employees must comply with all security and record keeping measures outlined in established policies and directives. Further, the Circular states that all FDIC records and data shall be protected against unauthorized disclosure, access, mutilation, obliteration, and destruction.

We contacted representatives of nine divisions and offices to determine if any had issued supplemental guidance specifically identifying data that should not be removed from the FDIC and used during telework sessions. Representatives of the five divisions and offices that responded indicated that they had not issued such guidance and were relying on existing corporate-wide guidance related to data security or encryption.

While DSC had not issued specific guidance related to data used during telework sessions, we noted that DSC had issued a memorandum dated August 15, 2006, entitled, *Safeguarding Examination Information* (Transmittal No. 2006-025), which states that examination information is broadly defined as all documentation involved in a bank examination. It includes the Report of Examination, examination work papers, and bank information received during the examination process. Attachment A of the memorandum states that the protection of examination information will require technical, physical, and administrative safeguards. The attachment states, for example, that all examination information stored on laptops, retained on CDs, DVDs, flash drives, or any other storage media shall be encrypted. Finally, the attachment states that staff on travel status or telework status must ensure confidential information is secure when unattended.

We also noted that DRR had issued guidance entitled, *DRR's Guidelines for Protecting Sensitive Data*, to help its employees and contractors better understand how to protect sensitive information. The guidelines describe: the types of data, when combined, which can be deemed as sensitive; responsibilities and methods for protecting sensitive information; and DRR systems that contain sensitive information.

Conclusion

The security goal of all federal agencies is to minimize the chance that unauthorized access to their network will occur. The FDIC continues to make progress in complying with OMB M-06-16 by identifying and resolving security weaknesses related to telework and remote access. Some risks remain associated with providing employees remote access to the FDIC's network and information systems. We are mindful in making recommendations as the FDIC faces similar challenges securing its information systems as do other agencies and must strike a balance between business needs, risk, and cost.

Recommendations

We recommend the Director, Division of Information Technology:

6. Pursue improvements in security controls associated with telework, when deemed cost effective, in the following areas:

- Continuing to work toward an enterprise-wide automated encryption solution for data stored on laptops, removable USB devices, and Personal Digital Assistants.

- Working to resolve technical issues that prevent FastAccess® with an open Outlook session from timing out after 30 minutes of inactivity in order to be consistent with the user re-authentication requirement of OMB Memorandum 06-16.

- Restricting user capability to extract and store sensitive data on non-FDIC computers while using RCN or FastAccess®.

We recommend the Director, Division of Administration:

7. Modify the FDIC Form 2121.5, *Employee/Supervisor Telework Program Agreement*, for regular or recurring telework situations to include identifying any sensitive data that may be used during telework and its source in order to assist management in making the decision to approve or disapprove a telework request.

OTHER MATTERS

INFLUENZA PANDEMIC PREPAREDNESS PLANNING

The Corporation's task force formed in February 2006 to develop the PIPP has neither completed the plan that will provide guidance for handling a pandemic event, nor has it set a target date for its completion.

To address the pandemic issue, the FDIC created a task force led by the Assistant Director, Facilities Operations Section. The task force is assigned to address the challenges of the pandemic influenza and to develop a PIPP that specifically includes preventive hygiene; social distancing or telework; and limiting movement in accordance with OPM's *A Guide to Telework in the Federal Government*. The PIPP is to be incorporated as an addendum to the FDIC Emergency Preparedness Plan.

According to task force members, the task force has:

- Drafted a "Decision Point" memorandum to the Human Resources Committee that the Assistant Director, Facilities Operations Section, expects to finalize by the end of September or early October;
- Conducted demonstrations of the Department of Treasury Web-based Pandemic Flu awareness-level training;
- Held discussions regarding a draft Pandemic Flu Plan;
- Participated in the Financial Banking Information Infrastructure Committee's pandemic flu table-top exercise.[8]

[8] The FBIIC and the Financial Services Sector Coordinating Council were responsible for conducting a pandemic flu exercise for the financial services sector in the United States from September 24 through October 12, 2007.

The Assistant Director confirmed that telework is the cornerstone of the FDIC's pandemic plan; however, he added that there are many telework-related issues that must be addressed before the PIPP is completed and implemented. For example, task force members are conducting discussions with FDIC management and union representatives to:

- Clarify Information Technology (IT) limitations and constraints, which include determining whether all employees can successfully activate their Safeword® authenticator tokens,
- Establish laptops in reserve for teleworkers,
- Ensure the FDIC population is telework-ready, and
- Determine how employees will be paid in a pandemic scenario.

While some progress has been made in developing the PIPP, additional management attention to the project may be beneficial to expediting its completion. Completing the PIPP and training FDIC managers and employees on its implementation will provide greater assurance that the FDIC can remain fully functional during a pandemic event.

Recommendation

We recommend the Director, Division of Administration:

8. Establish milestones for completing the FDIC's Pandemic Influenza Preparedness Plan and its incorporation, as an addendum, to the FDIC Emergency Preparedness Program.

SUBMISSION OF TELEWORK AGREEMENTS AND HOME SAFETY SELF-CERTIFICATIONS

The FDIC may be able to more efficiently administer the telework program. Specifically, the Corporation should pursue having employees participating in the FDIC telework program submit their Employee/Supervisor Telework Agreement (FDIC 2121/05) and their Home Safety Self-Certification (FDIC 2121/04) forms for approval and filing in an electronic format rather than in hard copy as currently required.

The FDIC has incorporated guidance from *A Guide to Telework in the Federal Government* regarding telework agreements and home safety self-certification into its Circular 2121.1 *FDIC Telework Program*. Section 5, *Program Guidelines,* of Circular 2121.1, states that supervisors must maintain a current form FDIC 2121/05 and form FDIC 2121/04. The supervisor is required to review these forms and keep a copy of each for their records. The Employee/Supervisor Telework Program Agreement provides needed contact information and outlines rights, responsibilities, and general program provisions. Section 8, *Responsibilities,* states that employees must update these documents annually or as otherwise required. Both forms are currently available electronically on the FDIC Intranet.

At our request, the FDIC's Legal Division reviewed the requirement for employees to submit FDIC 2121/05 and FDIC 2121/04. The Legal Division concluded that the requirement stems from negotiated provisions in the national Collective Bargaining Agreement (CBA) between the

FDIC and National Treasury Employees Union (NTEU), which states that both forms must be current and updated by January 31 of every calendar year.

Further, the FDIC's Legal Division stated that both the negotiated national CBA between the NTEU and the FDIC (at section 4E) and Circular 2121.1 (at section 8b), which was also negotiated with NTEU, require that employees participating in the FDIC telework program submit form 2121/04. This form is required to ensure that an employee's alternative work site complies with general safety standards and because an employee will be compensated under the Federal Employees Compensation Act if injured while actually performing official duties at the alternate work site.

As a result of its review, the Legal Division concluded that new requirements for electronic submission of forms 2121/05 and 2121/04 would be subject to negotiations with NTEU.

Recommendation

We recommend the Director, Division of Administration:

9. Evaluate the cost/benefit of employees electronically submitting forms 2121/05 and 2121/04, and if deemed cost-beneficial, negotiate with the NTEU to institute electronic submission and approval of the forms.

CORPORATION COMMENTS AND OIG EVALUATION

The DOA and DIT Directors provided a written response, dated November 29, 2007, to a draft of this report. The response is presented in its entirety in Appendix II. Management concurred with recommendations 1, 2, 3, 7, and 8, concurred with the intent of recommendation 4, and partially agreed with recommendations 5 and 6. Management did not agree with recommendation 9, but offered a reasonable explanation for not taking action on the recommendation at this time. A discussion of management's response to recommendations 5, 6, and 9 follows:

Recommendation 5: Implement periodic testing of equipment, technology, and technical support associated with large numbers of employees concurrently teleworking in an emergency situation and require individuals expected to telework in an emergency situation to periodically telework under non-emergency circumstances.

DOA deferred to DIT on this recommendation. DIT partially agreed with this recommendation and proposed an alternative action. DIT noted there is no requirement to support a large number of users to telework in an emergency. However, DIT agreed to stress test RCN, which is the most heavily used remote access method, to enhance the current engineering estimates of the projected number of users that can be supported on this technology.

DIT also noted that FDIC employees and contractors routinely use remote access tools to log into the FDIC network and that current usage results in thousands of remote connection sessions each month to the FDIC's network and systems, providing evidence that employees are capable of remotely accessing the network.

We accept DIT's alternative action to this recommendation; however, we continue to believe that it would be prudent to periodically require employees to practice telework under simulated emergency conditions. Doing so would also be consistent with FEMA and OPM guidance.

Recommendation 6: Pursue improvements in security controls associated with telework, when deemed cost effective, in the following areas:

- **Continuing to work toward an enterprise-wide automated encryption solution for data stored on laptops, removable USB devices, and Personal Digital Assistants.**

- **Working to resolve technical issues that prevent FastAccess® with an open Outlook session from timing out after 30 minutes of inactivity in order to be consistent with the user re-authentication requirement of OMB Memorandum 06-16.**

- **Restricting user capability to extract and store sensitive data on non-FDIC computers while using RCN or FastAccess®.**

DIT provided updated milestone information for the EEP project in November 2007. The FDIC completed Phase I encryption of all corporate laptops in November 2007. Regarding Phase II,

encryption of removable media, DIT provided a project plan with detailed milestones, which estimated completion of the encryption for USB drives in January 2008 and CDs by March 2008. Regarding Phase III encryption of PDA devices, DIT implemented a pilot in late November and anticipated full implementation of PDA encryption by the end of December 2007. This additional information is sufficient to address and close this portion of the recommendation.

DIT partially agreed with Bullet 2 above, regarding time-out of network sessions. DIT representatives were unaware of any technical solution that would prevent Outlook Web access from remaining open beyond the 30 minute time-out window when new email traffic is sent to the client by the exchange server. DIT agreed to complete an Acceptance of Risk memorandum by November 30, 2007 for this situation.

DIT partially agreed with Bullet 3 above, regarding logging data extracts and restricting downloads to non-FDIC computers. However, DIT representatives indicated that there is no tool in the current market place that will log data extracts and erase them after 90 days. DIT has implemented compensating controls to mitigate these risks. Further, DIT agreed to continue to look for and evaluate new solutions should they become available. The OIG considers DIT's response sufficient to resolve the recommendation.

Regarding restricting downloads to non-FDIC computers, DIT indicated that this is a risk for RCN, but not for Fast Access®. DIT is not aware of a solution to this situation, short of prohibiting access to the data, which DIT does not view as a viable business solution. DIT has made a business decision to accept this risk, and DIT has again agreed to complete an Acceptance of Risk memorandum by November 30, 2007.

The OIG considers the first portion of this recommendation (encryption) closed. The remaining portions of this recommendation (system time-out and logging of extracts/downloads of sensitive data) are resolved, but will remain open pending receipt of DIT Acceptance of Risk memoranda.

Recommendation 9: Evaluate the cost/benefit of employees electronically submitting forms 2121/05 and 2121/04, and if deemed cost-beneficial, negotiate with the NTEU to institute electronic submission and approval of the forms.

DOA did not agree with this recommendation. DOA indicated that the cost of the evaluation may exceed any savings derived from filing forms 2121/05 and 2121/04 electronically. DOA described the volume of paper generated through annual submissions as *de minimis*.

DOA also stated that, in the future, if such changes are to be determined to be in the Corporation's interest, they could be included as an agency proposal to be bargained over with NTEU when the national Collective Bargaining Agreement is next renegotiated. We accept management's decision on this recommendation, and we consider the recommendation closed.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to assess the extent to which the Corporation has established and implemented a telework program that is consistent with applicable federal standards and guidelines and recognized best practices. Prior to the start of our fieldwork, we met with senior officials of DIT, DOA, and OERM to ensure that our objectives and approach would result in information that addressed their needs and concerns.

Evaluation Methodology

To accomplish our objective, we became familiar with the FDIC's corporate policies and procedures applicable to the FDIC's telework program, including the FDIC BCP, which contains a BCP for each FDIC division and office and the Emergency Response Plan. Both documents are dated January 2007. We reviewed the FDIC's internal telework-related circulars, including the following:

- FDIC Circular 2121.1, dated May 2003, entitled, *FDIC Telework Program.* This circular establishes policy and issues guidance on the FDIC Telework Program within the FDIC.
- FDIC Circular 1380.3, dated April 1999, entitled, *Laptop Computer Assignments, Safeguards, and Asset Management.* This circular provides guidance on monitoring the movement of laptops within and outside of FDIC facilities.
- FDIC Circular 1360.9, dated April 2007, entitled, *Protecting Sensitive Information.* This circular establishes policy on protecting sensitive information collected and maintained by the Corporation and provides guidance for safeguarding the information.
- FDIC Circular 1500.5, dated January 2007, entitled, *FDIC Emergency Preparedness Program*. This circular provides guidance on responsibilities and guidelines for ensuring the safety and security of all FDIC personnel and the efficient resumption of the FDIC's critical business processes during an emergency.

Additionally, we compared and evaluated FDIC policy and program elements against applicable government-wide guidance from OPM, GSA, OMB, and FEMA as follows:

- Office of Personnel Management: OPM-II-A entitled, *A Guide to Telework in the Federal Government,* dated August 2006.
- General Services Administration: Federal Management Regulations (FMR) Bulletin 2007-B1 entitled, *Information Technology and Telecommunication Guidelines for Federal Telework and Other Alternative Workplace Arrangement Programs,* dated March 2007.
- Office of Management and Budget: OMB Memorandum M-06-16 entitled, *Protection of Sensitive Agency Information,* dated June 2006.
- FEMA, Federal Preparedness Circular (FPC) 65 entitled, *Federal Executive Branch Continuity of Operations,* dated June 2004.

We also reviewed relevant GAO reports and testimony.

On our behalf, KPMG reviewed:

- The National Institute of Standards and Technology, Special Publication 800-53 Rev. 1, *Recommended Security Controls for Federal Information Systems*, dated December 2006.
- FMR Bulletin 2007 B-1, *Information Technology and Telecommunications Guidelines for Federal Telework and Other Alternative Workplace Arrangement Programs*, dated February 2007.

Further, KPMG:

- Evaluated the FDIC's four methods of remote access,
- Interviewed program officials about the status of initiatives intended to identify methods of automated encryption of sensitive information stored on mobile computers and devices,
- Verified that the time-out function for the remote access methods functioned properly, and
- Assessed the FDIC's progress for logging data extractions and erasing them when no longer needed.

To identify "Best Practices" we reviewed guidance from 13 government agencies that included: the U.S Departments of Agriculture, Defense, Education, Energy, Homeland Security, Housing and Urban Development, Interior, Justice, Labor, State, Treasury, and the GSA, and the Securities and Exchange Commission. We also contacted the National Credit Union Administration and the Office of the Comptroller of the Currency to determine if their examiners were reported as teleworkers. We interviewed DOA's program officials about the status of the telework program, including the types of telework programs, participation levels by selected divisions and offices, and participation levels by grade.

We surveyed OERM, CU, DIR, DIT, DOA, DOF, DRR, DSC, and the Legal Division to determine if evaluations of the telework program had been conducted in their respective divisions and offices. All of the divisions and offices responded to our inquiry. We also surveyed the same divisions and offices to determine if they had issued supplemental guidance specifically identifying data that should not be removed from the FDIC and used during telework sessions. Five (DIR, DIT, DRR, DSC, and OERM) responded to this inquiry. We did not interview selected FDIC managers responsible for approving telework requests to understand what types of duties employees are performing while on telework. Neither did we interview managers to determine how they monitored employees' use of telework once we determined that neither DOA program officials nor the divisions and offices we surveyed had conducted an evaluation of the telework program. Additionally, we performed the following:

- Reviewed OPM telework reporting and verified the FDIC's compliance. We also interviewed OPM's Lead WorkLife Program Specialist to obtain clarification of OPM guidance regarding reporting of telework statistics;
- Performed analysis of telework participation information to identify trends and usage among divisions and offices. Furthermore, we evaluated the efficiency of the FDIC's use and management of telework program documentation;

- Assessed the FDIC's guidance on the types of applications that can be accessed and security category of information that can be processed, stored, and transmitted while teleworking and the FDIC's efforts to ensure information security at employees' telework locations; and
- Assessed the FDIC's policy and practices on providing equipment and infrastructure, including phone lines and information technology equipment to teleworkers.

We attended "Telework Made Easy" sponsored by the Mid-Atlantic Telework Advisory Council, which included a panel of experts from Microsoft, Dyscern, and the GSA who discussed how their organizations implemented an expansion of their telework efforts. Finally, we attended a hearing of the United State Senate Subcommittee on Oversight of Government Management, "Assessing Telework Policies and Initiatives in the Federal Government," which discussed new legislation, the Telework Enhancement Act of 2007 - S. 1000.

We performed our evaluation from June 2007 through September 2007, in accordance with the *Quality Standards for Inspections*.

CORPORATION COMMENTS

Federal Deposit Insurance Corporation
3501 Fairfax Drive, Arlington, VA 22226-3500
Division of Administration

November 29, 2007

MEMORANDUM TO: Stephen M. Beard
Deputy Assistant Inspector General for Audits

FROM: Arleas Upton Kea [Signed]
Director, Division of Administration

Michael E. Bartell [Signed]
Chief Information Officer and
Director, Division of Information Technology

SUBJECT: Management Response to the Draft OIG Evaluation Report Entitled, *Evaluation of the Federal Deposit Insurance Corporation's Telework Program (Evaluation No. 2007-019)*

This is in response to the subject Draft Office of Inspector General (OIG) Report, issued October 11, 2007. In its report, the OIG made nine recommendations.

We appreciate that the OIG noted that the FDIC's Telework Program is consistent in most respects with applicable federal standards and guidelines as well as recognized best practices. In addition, as noted in the Report, the FDIC Telework Program was recognized by the Telework Exchange as a recipient of its award for innovative use of technology in support of employees who telework and that "In OPM's 2006 Federal Human Capital Survey, FDIC employees reported an overall satisfaction rate of 56.3 percent with the Corporation's telework program compared to a rate of 21.8 percent government-wide." We also appreciate the OIG's acknowledgement of the Corporation's "extensive guidance on protecting sensitive information and implemented controls to address OMB and GSA information security requirements associated with teleworking," most notably two-factor authentication for user identification and encryption of remote network sessions. To continue providing a Telework Program for the benefit of the Corporation and its employees, we recognize that additional steps could be taken to enhance the overall program. This response outlines our planned corrective actions for each of the recommendations cited in the OIG's Report.

MANAGEMENT DECISION

Finding: Employee Participation in the FDIC's Telework Program

Recommendation 1: That the Director, Division of Administration (DOA) take steps to improve the quality and reliability of data collected for the purposes of determining the extent of telework participation by FDIC employees.

Management Response 1: DOA concurs with this recommendation.

Corrective Action: As noted in the evaluation, DOA currently uses the CHRIS T&A System to capture data to respond to the annual Telework Survey from OPM. The data collected includes each employee's name, division and office, grade, and the number of hours they teleworked during the year. The System reports data by pay period, not by the week or month. Given the more restrictive definition of telework established by OPM in 2005 that defined qualifying frequencies (i.e., 3 days a week, 1-2 days a week, or at least once per month), the FDIC was unable to respond fully on telework usage. Although 47% of FDIC employees participated in telework in 2006, the response to the Annual Survey captured only DSC Examiners who elected the Telework Option under the Telework Directive. FDIC participation was under-represented as the data could not be broken down to report the number of employees who teleworked 1-2 days per week or once a month based on the OPM definition of telework.

Additional guidance from OPM defining what constitutes a "day" of telework would be helpful in designing a report that is responsive to future surveys. Furthermore, since federal agencies collect time and attendance information by pay period and many agencies use these same systems to track telework, it makes sense for reporting requirements to mirror a pay period structure rather than asking for data by weeks and months. Since no federal employee works all 26 pay periods, the definition of a teleworker must take annual and sick leave, conferences, and training into consideration in order to gain a more accurate measure of teleworking.

We propose to collect more reliable data from CHRIS T&A by making the following assumptions:

- A "day" of telework is defined as 8 hours.
- A teleworker is defined as someone who teleworks one of the following schedules that roughly correspond to current OPM definitions: 6 or more days per pay period, 2 to 4 days per pay period, or 1 day during 2 consecutive odd and even pay periods.
- An employee is considered to be in telework status if they telework 21 out of 26 pay periods.

We will develop a new reporting format incorporating the assumptions described above and forward this request to Human Resources Information Management & Payroll for discussion and development. The reporting requirements will be implemented by March 31, 2008. In addition, we will request all time keepers to remind their employees by December 31, 2007 to properly code all telework.

Finding: Evaluation of the Telework Program

Recommendation 2: That the Director, DOA conduct an evaluation consistent with Circular 2121.1 to determine whether the FDIC's telework program is meeting management's expectations and desired outcomes. The evaluation could address, among other things:

- Whether goals and objectives exist against which the success and impact of the program can be measured,
- Fairness and consistency across the Corporation in how managers are administering the program;
- Sufficiency of leadership and management attention, and
- Extent of promotion, publicity, and training.

Management Response 2: DOA concurs with this recommendation.

Corrective Action: Notwithstanding a 47% telework participation rate for FDIC employees in 2006, DOA recognizes that evaluating the success and status of the FDIC Telework Program is a key factor in ensuring that the program is meeting the expectations of management and supporting the operational goals of the Corporation. DOA intends to define program goals and objectives for telework that would allow for meaningful program evaluations for telework in such areas as productivity, operating costs, employee morale, recruitment, retention, and business continuity and disaster recovery planning. These definitions will provide the framework for an evaluation tool designed to assess the progress of the FDIC telework program, identify problems and issues, and provide for appropriate adjustments and improvements. DOA anticipates that the first telework evaluation will be deployed by October 31, 2008.

Finding: Incorporating Telework into Business Continuity and Pandemic Preparedness

Recommendation 3: That the Director, DOA revise the FDIC BCPs and pandemic preparedness plans to more specifically describe the role telework plays in those plans.

Management Response 3: DOA concurs with this recommendation.

Corrective Action: The FDIC BCP is currently being revised with a January 2008 publication date. It will fully describe the role telework plays in all contingencies to include pandemic events. DOA anticipates completing the revised BCP by January 31, 2008.

Recommendation 4: That the Director, DOA identify personnel who would be expected to telework during an emergency and include corporate expectations into their telework agreements.

Management Response 4: DOA concurs with the intent of this recommendation and will address it with each Division.

Corrective Action: DOA will, as part of the BCP revalidation process, have Divisions identify personnel expected to telework during an emergency. DOA anticipates completing the revised BCP by January 31, 2008.

Recommendation 5: That the Director, DOA implement periodic testing of equipment, technology, and technical support associated with large numbers of employees concurrently teleworking in an emergency situation to periodically telework under non-emergency circumstances.

Management Response 5: DOA will defer to DIT on this response. DIT partially concurs with this recommendation.

Currently, there is no requirement to support a large number of users to telework in an emergency. Nevertheless, as an alternative to the recommendation, DIT infrastructure services will stress test RCN, which is the most heavily used remote access method, to enhance the

current engineering estimates of the projected number of users that can be supported on this technology.

It should be noted that FDIC employees and contractors routinely use the authorized remote access tools (RCN/WebVPN/Fast Access/Ascend Dial-in) to log into the FDIC network. Current usage results in thousands of remote connection sessions each month to FDIC's network and systems. Users of FDIC's remote services are well versed in the application of this technology. During the last 120 days, several thousand unique FDIC users have successfully taken advantage of this capability.

Corrective Action: DIT will stress test RCN capability by March 15, 2008.

Finding: Security Control Requirements for Telework

Recommendation 6: That the Director, Division of Information Technology pursue improvements in security controls associated with telework, when deemed cost effective, in the following areas:

- Continuing to work toward enterprise-wide automated encryption solution for data stored on laptops, removable USB devices, and Personal Digital Assistants,
- Working to resolve technical issues that prevent FastAccess with an open Outlook session from timing out after 30 minutes of inactivity in order to be consistent with the user re-authentication requirement of OMB Memorandum 06-16.
- Restricting user capability to extract and store sensitive data on non-FDIC computers while using RCN or FastAccess.

Management Response 6: DIT Response: Bullet 1: DIT considers this aspect of the recommendation resolved. Bullet 2 and 3: DIT partially concurs.

- 1st bullet: DIT recently completed phase I of the automated enterprise-wide effort encryption solution with the installation of encryption software on the new corporate laptops. DIT has active projects underway to deploy software that will encrypt portable devices. Following additional discussions with the OIG audit team, DIT provided the flash drive encryption project plan to OIG on November 15th and will provide the Request For Information (RFI) for the BlackBerry encryption to the OIG on November 23rd. Based on this discussion and the provision of this additional material, no further action is planned for this portion of the recommendation.

- 2nd bullet: Utilizing Fast Access, Outlook web access remains open and does not time out if the exchange server sends out new email traffic to the client within the 30 minute FDIC window. The session does however have a fixed maximum timeout at 180 minutes which partially mitigates this risk. FDIC knows of no further technical solution at this time to address this issue except, timing out and totally disconnecting the user at a 30 minute maximum session. This is not an acceptable business solution. The OIG audit team also indicated that they knew of no solution within our environment. DIT will continue to look for and evaluate new solutions if they become available. As an alternative action, DIT has made a business decision to accept this risk for business

purposes. DIT will complete an Acceptance of Risk memorandum by November 30, 2007.

- 3rd bullet: This is a two part issue. First, regarding 'logging data extracts and erasing extracts after 90 days', the current OIG report notes that DIT has implemented two compensating controls to mitigate the risk associated with this issue. Specifically, "the FDIC's Enterprise Information Management (EIM) group is restricting the ability to copy production data to non-production environments by implementing a set of procedures for data requests. EIM has also established a policy limiting access to production data for testing, quality control, and deployment preparation purposed to 45 days, at which point, access to the data is automatically removed." DIT research to date has concluded there is no tool in the current marketplace that will fully mitigate this issue. DIT will continue to look for and evaluate new solutions as they become available.

  The second part of the OIG's concern is that "RCN and FastAccess could allow users to store sensitive information unencrypted on home computers that are vulnerable to unauthorized access." DIT concurs that this is a risk for RCN but not for FastAccess. FastAccess does not provide the capability to download data to the user's PC. While DIT recognizes this risk, no solution short of prohibiting access to the data is available. Denying this access is not a viable business solution. As such, DIT has made a business decision to accept this risk for business purposes. DIT will complete an Acceptance of Risk memorandum by November 30, 2007.

Corrective Action: DIT agrees to document the acceptance of interim risk for bullets 2 and 3 above by November 30, 2007.

Recommendation 7: That the Director, DOA modify the FDIC Form 2121.5, *Employee/Supervisor Telework Program Agreement* for regular or recurring telework situations to include identifying any sensitive data that may be used during telework and its source in order to assist management in making the decision to approve or disapprove a telework request.

Management Response 7: DOA concurs with this recommendation.

Corrective Action: DOA will take steps to update FDIC Form 2121.5 to require the teleworker to identify any sensitive data and its source that may be used during telework. These changes create a new requirement that would be subject to negotiations with NTEU. DOA projects that the FDIC Form 2121.5 to the Telework Directive 2121.1 will be updated by March 31, 2008.

Finding: Influenza Pandemic Preparedness Planning

Recommendation 8: That the Director, DOA establish milestones for completing the FDIC's Pandemic Influenza Preparedness Plan and its incorporation, as an addendum, to the FDIC Emergency Preparedness Program.

Management Response 8: DOA concurs with this recommendation.

Corrective Action: The Pandemic Influenza Task Force (Task Force) has drafted a "Decision Points" Memorandum outlining key issues impacting FDIC's operations and personnel that will be submitted to the Human Resources Committee (HRC) for review and concurrence the week of November 19. The HRC's review of the "Decision Points" and Action Items contained within the memorandum is a precondition to the Task Force's finalization of the draft Pandemic Influenza Preparedness Plan (the Plan). DOA anticipates completion of the Plan and incorporation into the Business Continuity Plan by April 30, 2008.

Finding: Submission of Telework Agreements and Home Safety Self-Certifications

Recommendation 9: That the Director, DOA evaluate the cost/benefit of employees electronically submitting forms 2121/05 and 2121/04, and if deemed cost-beneficial, negotiate with NTEU to institute electronic submission and approval of the forms.

Management Response 9: DOA does not concur with this recommendation.

It is not clear that evaluating the cost/benefit of employees electronically submitting forms 2121/05 and 2121/04 would offset the amount of time and effort it would require to conduct such an assessment. It is worth noting that the annual requirement to submit telework forms generates a de minimis amount of paper. However, if such changes are determined to be in the Corporation's interest in the future, they could be included as Agency proposals to be bargained over with NTEU when the national Collective Bargaining Agreement is renegotiated.

Corrective Action: DOA does not propose any new corrective action in response to this recommendation.

If you have any questions regarding DOA's response, the point of contact is William Gately. Mr. Gately can be reached at (703) 562-2118. Any questions regarding DIT's response should be directed to Rack Campbell. Mr. Campbell can be reached at (703) 516-1422.

cc: Glen Bjorklund, DOA
Christopher Aiello, DOA
Gregory Talley, DOA
Michael J. Rubino, DOA
Brian Yellin, DOA
Tommie Barnes, DOA
Rack Campbell, DIT
James H. Angel, Jr., OERM

MANAGEMENT RESPONSE TO RECOMMENDATIONS

This table presents the management response on the recommendations in our report and the status of the recommendations as of the date of report issuance.

Rec. Number	Corrective Action: Taken or Planned/Status	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
1	Management concurred with the recommendation. DOA proposed a set of assumptions for collecting more reliable data from CHRIS T&A and agreed to develop a new reporting format for collecting telework participant statistics. In addition management agreed to request all time keepers to remind employees to properly code all telework.	March 31, 2008 December 31, 2007	$0	Yes	Open
2	Management concurred with the recommendation. DOA plans to define telework program goals and objectives that will allow for meaningful program evaluations for specific telework areas. The definitions will provide a framework for an evaluation tool designed to assess the progress of the FDIC's telework program, identify problems and issues, and provide for appropriate adjustments and improvements.	October 31, 2008	$0	Yes	Open
3	Management concurred with the recommendation and is currently revising the BCP to fully describe the role telework plays in all contingencies, including pandemic events.	January 31, 2008	$0	Yes	Open
4	Management concurred with the intent of this recommendation and as part of the BCP revalidation process, will have divisions identify personnel expected to telework during an emergency.	January 31, 2008	$0	Yes	Open

Rec. Number	Corrective Action: Taken or Planned/Status	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
5	Management partially concurred with the recommendation. DIT stated that there is no requirement to support a large number of users to telework in an emergency. As an alternative to the recommendation, DIT agreed to stress test RCN, which is the most heavily used remote access method. DIT also noted that current remote usage results in thousands of remote connection sessions each month that evidences employees' ability to work remotely. We accept management's proposal as a method to enhance the current engineering estimates of the projected number of users that can be supported on the FDIC's current technology.	March 15, 2008	$0	Yes	Open
6	Management considers the 1st bullet, associated with enterprise-wide encryption, resolved. DIT recently completed phase 1 of the automated enterprise-wide encryption solution with the installation of encryption software on new corporate laptops. DIT also provided or discussed with OIG the flash drive encryption project plan and the Request for Information for BlackBerry encryptions. DIT plans no further action on this portion of the recommendation. Management partially concurred with the 2nd bullet, associated with system time-out issues. DIT agreed that when using FastAccess, Outlook web access remains open and does not time out if the exchange server sends out new email traffic within the 30-minute FDIC time-out window. However, the session does have a fixed maximum time-out at 180 minutes that partially mitigates this risk. DIT knows of no acceptable business solution and will therefore complete an Acceptance of Risk memorandum.	N/A November 30, 2007	$0 $0	Yes	Open

Rec. Number	Corrective Action: Taken or Planned/Status	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
	Management partially concurred with the 3rd bullet, associated with logging data extracts and storing sensitive data on non-FDIC computers. DIT has concluded that there is no tool in the current market place that will log data extracts and erase them after 90 days. DIT has compensating controls designed to mitigate the risks. DIT has agreed to continue to look for and evaluate new solutions should they become available. The OIG considers this portion of the 3rd bullet closed. Regarding the second part of the 3rd bullet, DIT agreed that RCN does provide the capability to download data to a user's PC. However DIT is unaware of a viable business solution. DIT has made a business decision to accept this risk and DIT has agreed to complete an Acceptance of Risk memorandum. The OIG considers the first portion of this recommendation (encryption) closed. The remaining portions of this recommendation (system time-out and logging of extracts/downloads of sensitive data) will remain open pending receipt of DIT Acceptance of Risk memoranda. For tracking purposes, we will consider the overall recommendation to be open.	N/A November 30, 2007	$0 $0		
7	Management concurred with the recommendation. Subject to NTEU negotiations, DOA will update form 2121.5 to require the teleworker to identify any sensitive data that will be used during telework.	March 31, 2008	$0	Yes	Open

Rec. Number	Corrective Action: Taken or Planned/Status	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
8	Management concurred with the recommendation. The Pandemic Influenza Task Force has drafted a "Decision Points" memorandum outlining key issues impacting the FDIC's operations and personnel and submitted the memorandum to the Human Resources Committee for review. HRC review of the memorandum is a precondition of the Task Force's finalization of the draft Pandemic Influenza Preparedness Plan.	April 30, 2008	$0	Yes	Open
9	Management did not concur with this recommendation. DOA indicated that the time and effort necessary to evaluate the cost/benefit of employees electronically submitting forms 2121/05 and 2121/04 may not offset the proposed benefits. We accept management's decision to not take action on this recommendation.	N/A	$0	Yes	Closed

[a] Resolved – (1) Management concurs with the recommendation, and the planned corrective action is consistent with the recommendation.
(2) Management does not concur with the recommendation, but planned alternative action is acceptable to the OIG.
(3) Management agrees to the OIG monetary benefits, or a different amount, or no ($0) amount. Monetary benefits are considered resolved as long as management provides an amount.

[b] Once the OIG determines that the agreed-upon corrective actions have been completed and are effective, the recommendation can be closed.