Audit of
NARA's Telework Program

OIG Audit Report No. 11-20

September 30, 2011

Table of Contents

Executive Summary

The National Archives and Records Administration (NARA) Office of Inspector General (OIG) completed an audit of NARA's Telework Program. NARA developed the "Flexiplace" pilot program to comply with a mandate in allowing eligible NARA employees the opportunity to telework. Further, NARA implemented the Work-at-Home System (WAHS) to provide a remote access capability to teleworkers. During this audit, we assessed whether NARA is fully capitalizing on the identified benefits of telework and administering its telework program in accordance with Federal regulations and NARA policy.

Public Law 106-346 §359, *Department of Transportation and Related Agencies Appropriations Act, 2001* (the Appropriations Act), dated October 23, 2000, established a legislative mandate for Federal telework. The Appropriations Act requires each executive agency to establish a policy under which eligible employees of the agency may participate in telework to the maximum extent possible without diminished employee performance. Further, the Appropriations Act designates the Office of Personnel Management (OPM) as the lead in ensuring the requirements are applied to the entire Federal workforce. One of the tools OPM has promoted is the "Key Practices for the Implementation of Successful Telework Programs." Many of these key practices became legislatively mandated following the passage of Public Law 111-292, *Telework Enhancement Act of 2010*, which was signed into law on December 9, 2010.

Our review found that although NARA has had a pilot telework program in place since September 2001, the program does not fully encompass key best practices or facilitate the realization of identified benefits associated with teleworking. Further, the implementation of NARA's pilot telework program does not reflect key objectives of the agency's Transformation initiative. These conditions are due to inadequate managerial and administrative support of NARA's telework program. These same factors resulted in a lack of training, guidance, and assistance for telework supervisors, which have negatively impacted the overall implementation of NARA's telework program. The Telework Enhancement Act established many requirements that were due 180 days from its enactment. NARA is currently taking efforts to implement the long established key practices that have now become requirements; however, NARA is currently non-compliant with the Telework Enhancement Act.

Although OPM has identified benefits associated with telework, the practice invites risk and abuse if employees are not adequately trained, equipped, monitored and subject to appropriate supervision. These risk factors clearly exist at NARA.

Further, our review found that NARA's WAHS remains vulnerable to the threats it was designed to mitigate. The WAHS was not fully developed, tested, or administered in accordance with NARA policy and NIST security standards. Security requirements have not been met and in some cases remain untested. Now in full production, the WAHS is unnecessarily at risk of compromise, and controls in place to mitigate or detect such an event are insufficient.

Our audit identified several improvements to be made to NARA's overall telework program. We made a number of recommendations to more thoroughly ensure the telework program meets mandated requirements and improvements are made to the security of the WAHS.

Background

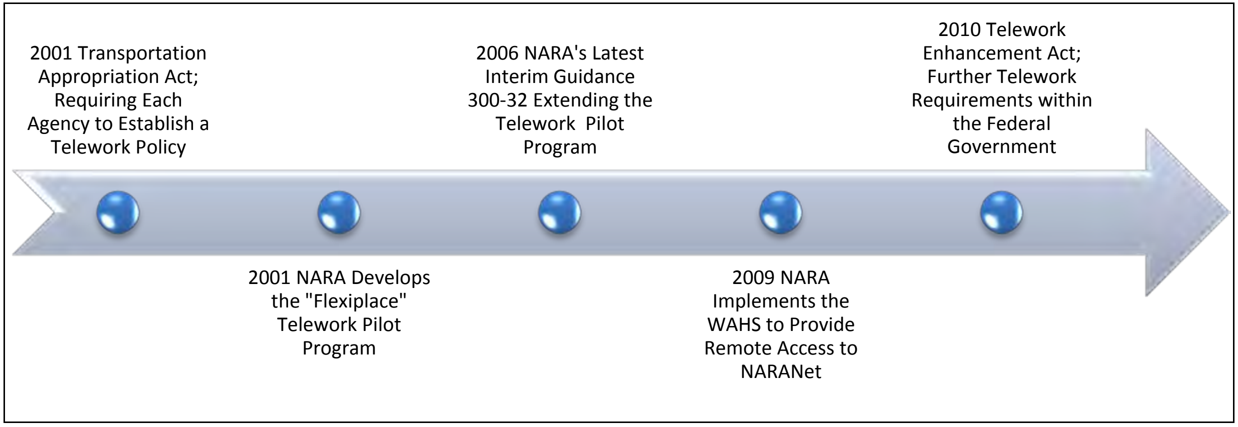
Over the past decade, telework programs have become increasingly widespread throughout the Federal Government. The Office of Personnel Management (OPM)—tasked by Congress to assist executive agencies in developing telework programs—defines telework as "work arrangements in which an employee regularly performs officially assigned duties at home or other worksites geographically convenient to the residence of the employee." Although addressed by various names (i.e., "telecommuting," "work at home," "flexible work," etc.), the general concept of telework within the Federal Government has been present and in use for many years.

In fiscal year 2001, the Department of Transportation and Related Agencies Appropriation Act (Public Law 106-346 §359) included a provision that required each executive agency to establish a policy under which eligible employees may participate in teleworking to the maximum extent possible without diminished employee performance. In complying with this requirement, on September 6, 2001, NARA issued interim guidance entitled "Flexiplace," establishing a pilot telework program within the agency. Due to the program's initial success, additional interim guidance was issued over the next five years to extend the pilot program and allow more offices within NARA to participate. The most recent interim guidance extending NARA's pilot telework program is dated August 8, 2006.

In mid 2007, NARA recognized a need to develop an enterprise-level remote access solution, in part, to support NARA's telework program. In August 2008, the Work-at-Home System (WAHS) began an initial pilot phase, followed by full operational capability in September 2009. The WAHS was designed to enable secure, remote access to selected General Support Systems (GSS) that reside on NARA's Network. The WAHS is licensed to support 250 concurrent teleworkers.

Most recently, Congress passed the Telework Enhancement Act of 2010, which was signed into law on December 9, 2010. The Telework Enhancement Act establishes additional requirements for Federal telework programs. Many of these requirements reflect key practices that were initially promoted by OPM and other agencies within the Federal Government (see Figure 1 for a timeline of these events).

Figure 1: Timeline of NARA's Telework Program


2001 Transportation Appropriation Act; Requiring Each Agency to Establish a Telework Policy
2001 NARA Develops the "Flexiplace" Telework Pilot Program
2006 NARA's Latest Interim Guidance 300-32 Extending the Telework Pilot Program
2009 NARA Implements the WAHS to Provide Remote Access to NARANet
2010 Telework Enhancement Act; Further Telework Requirements within the Federal Government

Objectives, Scope, Methodology

The overall objective of this audit was to determine whether NARA is fully capitalizing on the identified benefits of telework and administering its telework program in accordance with Federal regulation and NARA policy. Our review focused on whether NARA management was aligning its telework program to meet established and recently enhanced Federal telework requirements. Further, this audit covered the implementation of NARA's telework program in terms of supervisory involvement and information security.

To accomplish our objective, we interviewed key NARA personnel from the Office of Administration[1] and the Office of Information Services and examined NARA policies governing its telework program. We gained an understanding of NARA's documentation and approval process for establishing individual telework arrangements. We reviewed program documentation for NARA's Work-at-Home System (WAHS) in regards to information security. Further, we met with a sample of telework supervisors and teleworkers from offices throughout the agency to observe and gain an understanding of the actual implementation of the telework program. We compared the implementation of the telework program to NARA's policy. In addition, we compared NARA's telework policy and WAHS to applicable Federal regulation and other telework guidelines, specifically: the Department of Transportation and Related Agencies Appropriation Act, 2001 (Public Law 106-346 §359); The Telework Enhancement Act of 2010 (Public Law 111-292); National Institute of Standards and Technology (NIST) SP 800-46, *Guide to Enterprise Telework and Remote Access Security*; Office of Personnel Management (OPM), *Guide to Telework in the Federal Government*; Government Accountability Office (GAO)-04-950T, *Human Capital: Key Practices to Increasing Federal Telework*; and GAO-03-679, *Human Capital: Further Guidance, Assistance, and Coordination Can Improve Federal Telework Efforts*.

Our audit work was performed at Archives II in College Park, Maryland; Archives I in Washington, DC; and various telework alternative work locations throughout Maryland. The audit took place between February 2011 and July 2011. We conducted this audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[1] NARA underwent a Transformation effort during the timeframe of this audit. Office names and symbols have subsequently changed to reflect the reorganization. However, the previous office names and symbols are used in the body of this report to reflect the historical names of the offices involved throughout the development of the telework program, as well as to remain consistent with the office names used in applicable NARA policy. Recommendations are addressed using the most current office and management titles.

Audit Results

1. Overall Management of NARA's Telework Program Lacking

Although NARA has an established pilot telework program, the program does not fully encompass key best practices or facilitate the complete realization of identified benefits associated with teleworking. These conditions exist because NARA has not provided adequate managerial and administrative support, nor significantly updated or promoted its nearly decade-old interim guidance—despite ever increasing emphasis on telework throughout the Federal Government. As a result, NARA's telework program must try to catch-up to well established best practices that have now become legislatively mandated telework requirements. Additionally, in delaying action until now, NARA has missed opportunities to further reduce costs, increase resiliency and preparedness, and enhance the quality of employee work-life.

Public Law 106-346 §359, *Department of Transportation and Related Agencies Appropriations Act, 2001* (the Appropriations Act), dated October 23, 2000, provides the initial legislative mandate for Federal telework. The Appropriations Act requires each executive agency to establish a policy under which eligible employees of the agency may participate in telework to the maximum extent possible without diminished employee performance. The conference report for the Appropriations Act provides additional detail on this requirement, stating "each agency participating in the program shall develop criteria to be used in implementing such a policy and ensure that managerial, logistical, organizational, or other barriers to full implementation and successful functioning of the policy are removed. Each agency should provide for adequate administrative, human resources, technical, and logistical support for carrying out the policy." Further, the Appropriations Act designates the Office of Personnel Management (OPM) as the lead in ensuring the requirements are applied to the entire Federal workforce.

In this capacity, OPM assists agencies in developing policy and reports on telework progress, guidance, and best practices. OPM's telework website (telework.gov) contains a number of tools and resources to aid agencies in staying abreast of the evolving telework best practices. Specifically, OPM has adopted "Key Practices for the Implementation of Successful Telework Programs" (see Appendix A for the complete list). These key practices, which were first identified by the U.S. Government Accountability Office (GAO) in July 2003, are divided into seven categories that range from planning to program evaluation.

In an initial effort to comply with the telework requirements of the Appropriations Act, NARA issued Interim Guidance 300-13, *Flexiplace*, on September 6, 2001. In addition to establishing a pilot telework program within NARA, the guidance details responsibilities, participation eligibility, standards of conduct, and other requirements of the program. Minor updates were made to NARA's interim guidance over the years; however, the majority of the policy has remained unchanged.

During our review—while examining NARA's telework policy and program implementation and administration—we identified a number of key practices that had yet to be incorporated into

NARA's telework program. These unimplemented key practices are described under the seven categories below.

- **Program Planning.** Until recently, NARA had not established a telework coordinator. According to OPM, this is the first of many important steps in planning for an effective telework program. Further, NARA has not established a cross-functional team, which has resulted in the separate development of the telework program and the Office of Information Services (NH) Work-at-Home System (WAHS). Proper funding is also necessary for an effective telework program. Officials from the Office of Administration (NA) stated funding has not been sufficient to meet the needs of NARA's telework program. NA officials estimate they only have funding for one quarter of a full time equivalent (FTE) devoted to the telework program, however, they estimate it requires at least one FTE

- **Telework Policy.** A major component of an effective telework policy includes developing a telework agreement for use between all teleworkers and their managers. NARA's pilot telework policy only requires telework agreements to be established between teleworkers who participate on a recurring basis. Ad hoc teleworkers are not currently required to sign an agreement. Further, in order for the policy to be effective, it should be free from ambiguity and redundancy. NARA's policy contains conflicting and unclear statements; examples include the number of telework days allowed and whether or not Senior Executives may participate.

- **Performance Management.** GAO reported that agencies need to establish guidelines to minimize adverse impacts that telework can have on non-teleworkers before employees begin to work at alternative worksites. Although NA has identified this as a scenario that is present at NARA—which negatively impacts telework participation—guidelines to minimize the adverse impact on non-teleworkers have not been established.

- **Managerial Support.** GAO identified that it is critical to obtain support from top management and to address managerial resistance in establishing an effective telework program. Based on interviews with telework personnel, coupled with the historically slow growth of telework participation within NARA, further improvement in management support is needed. OPM encourages agencies and managers to be creative in considering the use of telework; it should not be an "all or none" proposition. OPM guidance further states most, if not all, jobs include some duties that are considered "portable" and do not necessarily require the employee to be physically present at the regular worksite.

- **Training and Publicizing.** OPM's key practices state, at a minimum, telework training should be provided to managers and teleworkers. According to NA personnel, NARA has offered very little training related to telework. NA officials stated an indirect effort to promote telework involved requiring NARA employees to differentiate telework from duty station work on their timesheets; however, again citing lack of resources, NA stated very few specific telework promotional activities have taken place.

- **Technology.** OPM key practices report agencies should conduct an assessment of teleworker and organization technology needs. Further, the key practices include providing technical support for teleworkers. NA and NH did not establish a cross-functional team to determine the requirements for NARA's WAHS. As a result, required capabilities did not fully reflect actual needs. In addition, NARA telework policy is ambiguous in terms of whether or not NARA provides technical support to teleworkers, stating "the employee installs, services, and maintains any personal equipment and furniture to be used." NARA does not specifically mention technical support in its telework guidance.

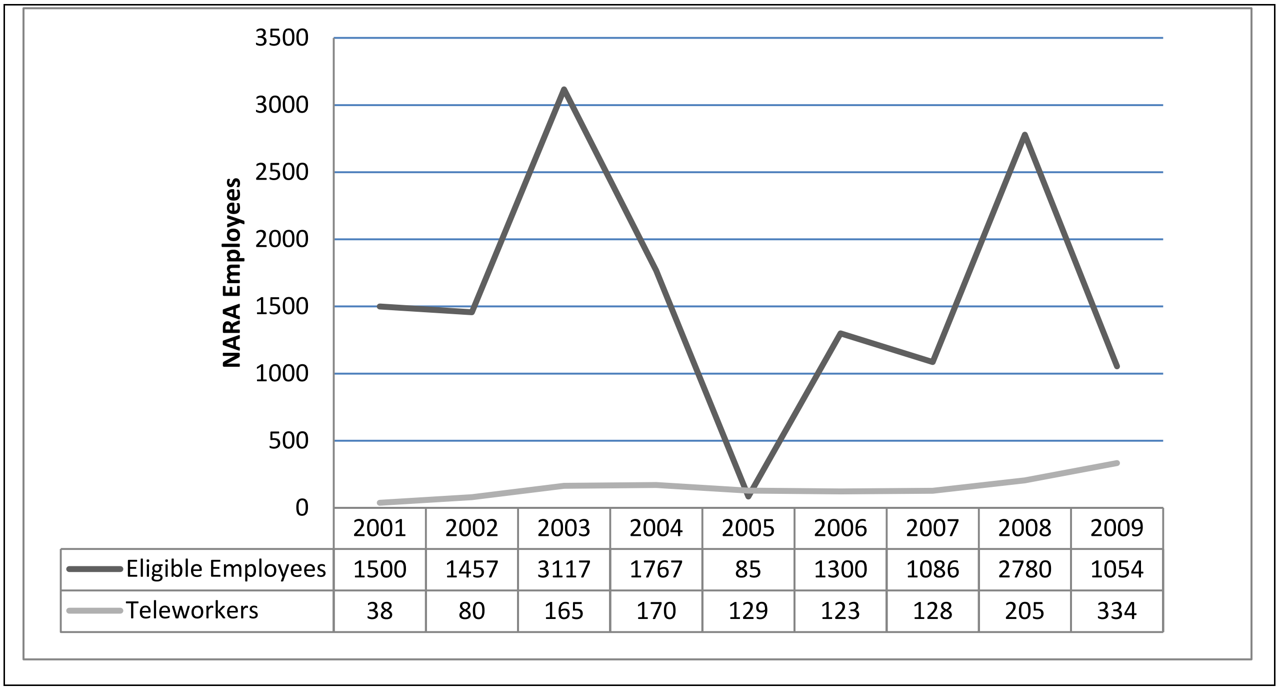
- **Program Evaluation.** GAO reported that agencies should develop program evaluation tools and use such tools from the very inception of the program to identify problems or issues with the program and to develop an action plan to guide any necessary changes. In addition, the key practices include tracking participation numbers with a reliable system. NARA has not established consistent processes, procedures, or tracking systems to collect data to evaluate the telework program. Further, until recently, NARA has not used a reliable system to track telework participation.

Regular attention by agencies to the key practices is important to foster program growth and remove barriers to telework participation. For example, in 2002, OPM had already reported that training was by far the most frequently cited tool for expanding telework participation and addressing the wide array of telework barriers and concerns. However, as mentioned above, telework training has yet to be fully utilized at NARA. The results of not fully implementing well established telework key practices is reflected in the relatively flat growth in number of NARA employees participating in the telework program over the years.

Management of NARA's Telework Program

Around the time NARA established its initial pilot telework program in September 2001, NA began providing OPM with data related to NARA employee participation and other progress measurements. OPM compiles this information from each agency on an annual basis and then reports to Congress on the status of telework in the Federal Government. The chart below depicts the data NARA provided to OPM—as reported in OPM's annual status reports—including the number of staff eligible to telework and the number of actual teleworkers at NARA (see Figure 2).

Figure 2: NARA's Input to Annual OPM Data Calls Reported to Congress



	2001	2002	2003	2004	2005	2006	2007	2008	2009
Eligible Employees	1500	1457	3117	1767	85	1300	1086	2780	1054
Teleworkers	38	80	165	170	129	123	128	205	334

Although NA has recently implemented a more scientific method of tabulating telework data within NARA, the chart above provides a historical perspective of the level of management afforded to reporting NARA telework data to OPM. When asked about the fluctuations in number of NARA employees eligible to telework from year to year, NA personnel stated “bad data” was reported in some years. Other factors may include discrepancies in calculation methods. This data is also used in measuring goals of overall telework participation levels. NA personnel stated the participation goal of NARA’s telework program is to have at least 15 percent of eligible employees telework. However, without consistent eligibility criteria or measuring methods, NARA cannot reasonably determine if it is meeting its goal. For example, the last two years of data reported indicate participation levels jumped from 7 percent to 32 percent. Although there was notable growth in telework participation during this period, the increased participation rate is exaggerated by a drastic reduction in the number of telework eligible staff reported.

In terms of overall management of NARA’s telework program, NA personnel stated until recently, NARA did not have a designated telework coordinator or any other staff specifically dedicated to the management of the program. OPM guidance states each agency should designate a telework coordinator who acts as the key contact for policy and program questions. Further, OPM guidance instructs managers and teleworkers to maintain frequent contact with their telework coordinator to ensure the agency’s policy and procedures are properly applied and to ensure awareness of the full range of support and resources available. During the entrance conference with NA, management was unable to identify the NARA staff member listed on the OPM telework website as the Telework Coordinator for NARA’s program. Further, the phone number listed on NARA’s most recent Interim Guidance is outdated and does not belong to the person listed, nor does it belong to the person currently responsible for providing telework assistance. NA cited turnover and insufficient resources for the reasoning behind the current management state of NARA's telework program.

Management of NARA's Telework Policy

Another basic tenet of a successful telework program involves developing an agency-wide telework policy. NARA issued Interim Guidance 300-13, *Flexiplace,* on September 6, 2001. The purpose of this initial guidance was to establish a pilot telework program at NARA for a six-month period beginning on October 1, 2001. Based on the success of the initial telework program, an extension of the pilot was granted on three separate occasions through the issuance of the following revised interim guidance:

- Interim Guidance 300-21, *Flexiplace*, dated November 14, 2002;
- Interim Guidance 300-28, *Flexiplace*, dated October 19, 2005; and
- Interim Guidance 300-32, *Flexiplace*, dated August 8, 2006.

All three updates made to NARA's telework guidance state the same purpose, which is to extend the pilot program. Apart from revisions to eligibility qualifications and the number of specifically identified NARA offices allowed to participate in recurring telework, very few changes have been made in comparison to NARA's initial version issued in September 2001. Furthermore, the telework agreement and arrangement forms—which are used to document telework agreements between managers and teleworkers—have remained unchanged for nearly ten years, and contain references to outdated policy.

Although many key telework best practices were identified by OPM and GAO as early as July 2003, NARA's subsequently issued revised interim guidance did not reflect these key practices. Furthermore, after nearly a decade, NARA's telework program remains in a pilot phase, and the guidance remains "interim." NA management recognizes that the telework policy needs to be revised, stating in one meeting "even the name 'Flexiplace' is outdated." NA officials stated they are in the process of revising the telework policy.

Increased Emphasis on Telework

Over the last few years, NARA's telework program has remained relatively stationary, with few updates to the policy, minimal promoting and training, and little overall management attention. However, during the same timeframe, telework practices were evolving more drastically elsewhere in the Federal Government. Apart from the key practices identified earlier, OPM's annual reports to congress have consistently provided lessons learned and additional guidance based on information canvassed from agencies throughout the Federal Government. Further, OPM has provided updated guides on teleworking, which outline practical information to assist agencies in implementing telework programs.

Increased emphasis on telework has been observed at all levels of the government. In March 2010, the President hosted a White House Forum on "Work-Life Balance and the Economics of Workplace Flexibility." The forum identified evidence supporting a potential boost in productivity and morale as a result of implementing flexible workplace practices. Other benefits associated with flexible workplace arrangements identified include improved employee health and decreased absenteeism—a major cost for employers. The forum report concluded by stating "…it is critical for the 21st century U.S. workplace to be organized for the 21st century workforce."

Furthermore, through a number of legislative actions, Congress has promoted telework programs in an effort to further accomplish a number of positive outcomes. This culminated in the passage of the Telework Enhancement Act of 2010, which was signed into law on December 9, 2010. The Telework Enhancement Act legislatively mandates many of the key practices identified early on by OPM and GAO. Some of which include:

- Designating a Telework Managing Officer;
- Notifying all employees of the agency of their eligibility to telework;
- Requiring all teleworkers to have a written agreement;
- Ensuring that an interactive telework training program is in place for all eligible employees, managers, and teleworkers;
- Purchasing computer systems that enable and support telework;
- Submitting data to OPM reporting on the degree of telework participation; and
- Setting and reporting on telework related goals.

Now that these key practices have become mandatory, NARA must ensure compliance. The majority of the requirements contained within the Telework Enhancement Act were to be implemented by June 7, 2011 (180 days after the act was signed into law). NA officials stated they were in the process of updating NARA's telework policy and implementing the newly mandated requirements of the Telework Enhancement Act. However, as of the June 7, 2011 deadline, NARA has yet to issue revised policy or guidance pertaining to its telework program. NA personnel stated they expect the policy to be issued shortly.

Implications of Delayed Action

OPM and agencies throughout the Federal Government have identified and reported numerous benefits associated with teleworking, some of which include:

- Assists with recruiting and retaining the best possible workforce,
- Ensures continuity of operations and maintains operations during emergency events,
- Promotes management effectiveness by targeting reductions in management costs related to employee turnover and absenteeism,
- Reduces real estate costs, transit costs, and environmental impact,
- Enhances work/life effectiveness and balance, and
- Allows employees to better manage their work and family obligations, thereby retaining a more resilient, results-oriented workforce better able to meet agency missions and goals.

On June 8, 2011—the day after many of the Telework Enhancement Act requirements went into effect—representatives from the Nuclear Regulatory Commission (NRC) and the General Services Administration (GSA) spoke at a forum detailing the benefits of telework realized at their respective agencies. The representatives noted that it was not a coincidence that their agencies had well established telework programs and also ranked in the top-ten of OPM’s annual Federal Employee Viewpoint Survey in terms of employee satisfaction (NRC: first place; GSA: seventh place). In contrast, NARA—with its less developed telework program—is currently tied for last place in a ranking conducted by the Partnership for Public Service. Although telework is only one factor, with the passage of the Telework Enhancement Act, NARA must ensure it is thoroughly addressed. Until NARA devotes the resources and attention necessary to implement its telework program consistent with mandates and key practices, the agency will continue to delay the full realization of identified telework related benefits and remain non-compliant with the Telework Enhancement Act. Offering employees the opportunity to telework can result in heightened job satisfaction. If properly instituted at NARA, teleworking can help support NARA's transformation initiative of making NARA "A Great Place to Work."

Recommendations

1. We recommend the Chief Human Capital Officer (H):

    a. Revise NARA’s telework policy and implement NARA’s telework program to incorporate OPM and GAO’s “Key Practices for the Implementation of Successful Telework Programs.”
    b. Monitor compliance with deadlines and requirements established in the Telework Enhancement Act.
    c. Establish a cross functional team with the Office of Information Services (I) to ensure remote access capabilities will meet increased NARA telework demands and to ensure appropriate security guidance is included in NARA telework policy.
    d. Develop a method and common criteria for tracking telework participation.

Management Response

Management concurred with the recommendations.

2. NARA’s Telework Guidance not Consistently Implemented

Our review revealed a number of telework supervisors did not consistently and properly implement NARA’s telework program in accordance with NARA policy and OPM guidance. This occurred due to an overall lack of telework training, misunderstanding of telework guidance and forms, and confusion as to who NARA’s telework coordinator is and how to obtain additional assistance regarding NARA’s telework program. As a result, telework is not always conducted appropriately and required telework supervision and management is often not achieved.

NARA Interim Guidance 300-32, *Flexiplace*, dated August 8, 2006, is the most recent version of NARA’s telework policy. Like previous versions, the policy incorporates telework supervisor responsibilities. The main supervisory responsibilities include approving, disapproving, or terminating telework arrangements, as well as, monitoring teleworker productivity and performance. To further facilitate these responsibilities, NARA’s telework policy contains a number of documentation requirements. The forms used in support of NARA’s telework program include the following:

- NA Form 3038, *Request for Ad Hoc Flexiplace Arrangement*—for teleworkers participating on an ad hoc basis, this document describes the hours or days being requested, the specific assignments or projects to be worked on during the period away from the office, and the products or progress that can reasonably be expected to be accomplished during the period away from the office. The form must be submitted and written supervisor approval granted prior to the ad hoc telework commencing and signed again upon review of the accomplishments documented at the completion of the telework.

- NA Form 3039, *Request for Recurring, Scheduled Flexiplace Arrangement*—for teleworkers participating on a recurring basis, this request form contains the telework employee’s name and occupational information, expected duration of proposed telework arrangement, specific work schedule, and other evaluation information. The form must be submitted and approved by the office head and the employee’s immediate supervisor prior to the recurring telework commencing.

- NA Form 3040, *Flexiplace Agreement*—NARA’s Interim Guidance requires telework candidates to enter into this agreement prior to beginning a recurring telework schedule. The form documents the duty station, alternative workplace, and work schedule, and includes additional requirements that must be met by the teleworker and supervisor. Once completed, the form must be signed and retained by both the telework employee and supervisor.

- NA Form 3041, *Self-Certification Safety Checklist for Home-Based Flexiplace Participants*—this form, completed by the telework candidate, provides a level of assurance that the alternative workplace proposed is a safe work environment. The form includes the employee’s work address and alternate worksite location, as well as a questionnaire related to the workplace environment and computer workstation. The form

> must be submitted and receive supervisory approval before either ad hoc or recurring telework may commence.

In addition to NARA policy, OPM's "Guide to Telework in the Federal Government," provides insight on how to be an effective telework manager. The guidance states the teleworker and manager should enter into a written agreement for every type of telework, whether the employee teleworks regularly or ad hoc. The written agreement provides a framework for the discussion that needs to take place between the manager and teleworker about expectations. Further, OPM states telework agreements are "living documents" that should be revisited by the manager and teleworker and re-signed regularly, preferably at least once a year. The guidance states management expectations of a teleworker's performance should be clearly addressed in the telework agreement. Lastly, as with onsite employees, teleworkers must be held accountable for the results they produce.

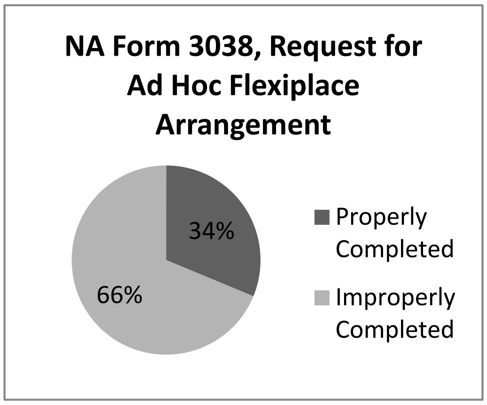
In performing our review, we interviewed 19 telework supervisors from nine different offices within NARA and requested the telework documentation of the over 100 telework staff they collectively supervise. The documentation sampled represented nearly one third of all NARA teleworkers. In addition, we interviewed and observed five teleworkers from their respective alternative worksites. Based on our interviews and observations, and our analysis of telework documentation, we determined a number of telework supervisors did not consistently and properly implement NARA's telework program in accordance with NARA policy and OPM guidance. Specifically, many of the controls put in place to promote oversight, accountability, and productivity were not fully applied by all telework supervisors.

For example, one basic telework supervisor oversight and accountability practice involves maintaining an awareness of employee work schedules. Both NARA Interim Guidance 300-32 and NA Form 3040 require the employee to either 1) log in and log out each workday via e-mail to their supervisor, or 2) complete a self-certification statement if they log in and log out by telephone. Despite this requirement, not all supervisors interviewed required their telework staff to directly e-mail workday log ins and log outs. Further, when asked, not all telework staff were aware of this requirement.

NA Form 3038, *Request for Ad Hoc Flexiplace Arrangement* contains a built in control related to accountability and productivity. The top half of the form includes information related to the expected work to be conducted while teleworking. The bottom half of the form, which is completed after the telework has taken place, describes the actual work accomplishments. The supervisor is required to sign off both prior to the telework and once again after the telework is completed. NARA policy requires that supervisors retain these completed forms for at least one year. However, a number of NA Forms were either not signed in a timely manner or all together missing from the samples we requested.

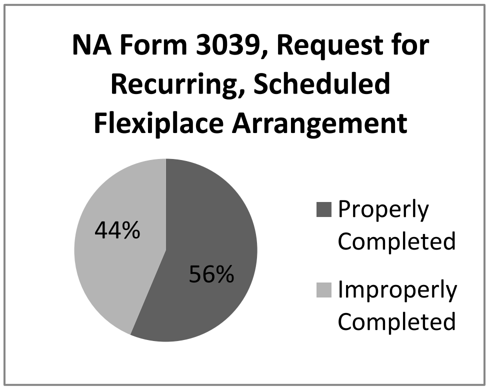
In addition, comparisons of the telework documentation provided by the supervisors and NARA's remote user access log further substantiate non-adherence to the aforementioned controls. Although most supervisors stated that sign in/out e-mail procedures were implemented within their respective offices, access logs identified a number of teleworkers did not access their e-mail within the surrounding hours of their scheduled telework. A number of factors may have contributed to employees not sending e-mails, including access and IT problems; however, in situations where an e-mail cannot be sent, NARA policy requires the employee to call their supervisor and complete a self-certification statement. Furthermore, in terms of retaining documentation supporting approval, the remote access log indicated telework was performed more often than the supervisor provided support documentation indicated.

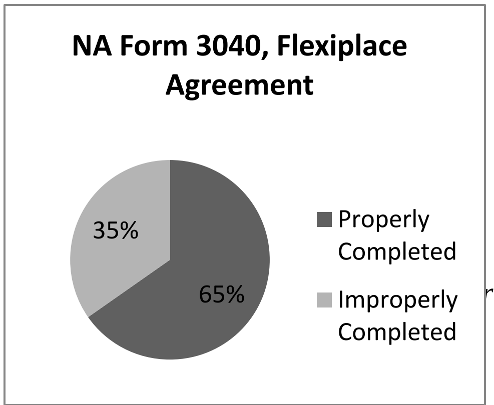
Further, we identified numerous situations in which supervisors approved incomplete or inaccurate telework documentation, or allowed telework to take place prior to having their staff complete the required agreements and forms. Analysis of the four standard telework forms and the identified deficiencies pertaining to each are described below.



During the review, we obtained documentation for teleworkers who participated on an ad hoc basis. Of the 32 ad hoc teleworkers sampled, 21 (or 66 percent) had improperly completed NA Form 3038, *Request for Ad Hoc Flexiplace Arrangements* (see chart on the left). A number of the NA Form 3038s were not approved prior to the telework taking place. Others did not provide explanations of the specific assignments or projects expected to be worked on during the time period away from the office and some had blanket approval that spanned months without listing specific dates for the ad hoc work to take place. Further, a number of the forms provided generic accomplishment responses and supervisors often did not sign off on the forms in a timely manner once the telework was completed.

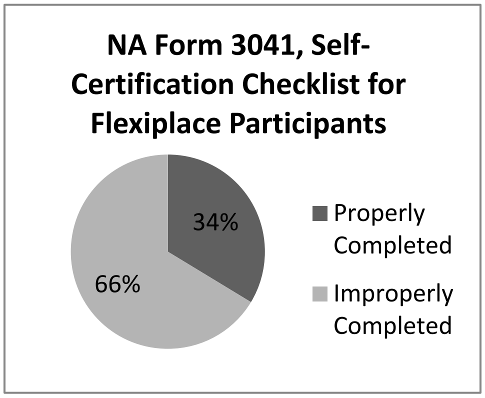
In addition, we obtained documentation for 71 teleworkers who participated on a recurring basis. Of those sampled, 31 teleworkers (or 44 percent) had improperly completed NA Form 3039, *Request for Recurring, Scheduled Flexiplace Arrangements* (see chart on the right). Examples of the issues observed include: unsigned and unapproved arrangements, arrangements with up to four days per week of telework without special approval, arrangements that had surpassed their durations by up to two years, arrangements that did not include the location of the offsite workplace, arrangements with an offsite work location listed as a post office box or that did not match the location listed on other documents, and arrangements in which work schedules did not match those listed on other documents.





Although OPM guidance stipulates all teleworkers should sign an agreement, NARA policy only requires agreements for employees who telework on a recurring basis. Of the 71 NA Form 3040, *Flexiplace Agreements* reviewed, 25 (or 35 percent) were improperly completed (see chart on the left). Examples of the issues identified include: agreements that had not been updated in over four years, agreements that were not signed or dated, agreements that did not include work schedules or the address of the alternative workplace, and agreements that were incomplete or altered to remove pertinent data.

Further, NARA policy requires all teleworkers (regardless of ad hoc or recurring) to complete a NA Form 3041, *Self-Certification Checklist for Home-Based Flexiplace Participants*. However, not all sampled NARA teleworkers had completed the checklist. Of the 95 available for review, 63 (or 66 percent) had completed NA Form 3041 improperly (see chart on the right). Examples of the issues observed include: forms that did not contain the address of the location being self-certified, forms that were not signed or dated, supervisors that were unaware that checklists had to be completed by employees teleworking on an ad hoc basis, and telework allowed prior to obtaining an approved checklist.



Overall Lack of Telework Training

OPM identified training as the most frequently cited tool for addressing telework concerns. Further, OPM has highlighted how telework training has increased the success of telework programs at other agencies. However, during our interviews with teleworkers and telework supervisors, none were aware of or could recall participating in telework specific training. NA officials acknowledged, due to a lack of resources, there has not been an organized effort to train telework managers and staff.

The Telework Enhancement Act has established new requirements related to telework training. According to the Act, agencies must ensure that an interactive telework training program is provided to all managers and all eligible telework employees. Further, employees must successfully complete the interactive training before entering into a written agreement to telework.

Misunderstanding of Telework Guidance and Forms

OPM guidance states telework policy for each agency should be designed and written to serve as a useful, practical resource to telework employees, managers, supervisors and others with a need to know about the agency's telework program. Further, OPM recommends the policy be organized logically and avoid the use of ambiguous terms and redundancies. Although most telework supervisors stated they relied almost exclusively on NARA's telework policy to implement the telework program within their respective offices, the inconsistencies between offices highlighted a number of misunderstandings regarding the telework policy. For example, some supervisors were unsure which forms applied to each type of telework situation, in some cases this resulted in teleworkers not completing the required forms.

Further, NARA's policy contains a number of ambiguous and redundant requirements. For example, in terms of the number of days per week an employee can participate as a recurring teleworker, NARA's policy offers three different answers: 1) one or more days per week, 2) up to two days per week, and 3) typically less than half of the employee's official duty station in any given pay period. Similarly, NARA's limit on the number of days an employee can telework ad hoc is equally ambiguous, the policy states the following: 1) the employee typically works for a day or two, 2) no more than two day-long periods or equivalent time during a pay period, and 3) as long as your supervisor is satisfied with your performance during these occasional ad hoc periods (typically no more than one ad hoc period during a given pay period), there is no limit to the number of ad hoc periods you may work.

Another concept interviewed supervisors were unsure about pertained to whether or not Senior Executives were permitted to telework. NARA's policy does not specifically address this issue. However, OPM states managers and supervisors must be committed to using telework to the fullest extent possible if Federal telework programs are to succeed. OPM—citing research in the work/life field—states supervisors, managers and senior executives who model the use of workplace flexibilities such as telework in any organization serve as key drivers in effecting positive cultural change in that organization.

Limited Awareness of Available Telework Guidance and Assistance

OPM and GAO best practices have long established that agencies should designate a Telework Coordinator who acts as the key contact for policy and program questions. Further, OPM states managers should maintain frequent contact with the Telework Coordinator to ensure the agency's policy and procedures are properly applied and to ensure full awareness of the range of support and resources available. However, during our interviews of teleworkers and supervisors, we asked if anyone was familiar with NARA's Telework Coordinator. Only one of the interviewees was able to identify NARA's Telework Coordinator and many were unaware that there was even such a position at NARA. These responses were expected, as NA had only recently officially assigned the Telework Coordinator position.

With the enactment of the Telework Enhancement Act, agencies are now required to designate a Telework Managing Officer. The Telework Managing Officer will take on the role of serving as the primary point of contact for policy and program questions. OPM guidance recommends telework staff that have questions or issues should now direct their concerns to the Telework Managing Officer. In addition, the Telework Managing Officer will be a senior official with direct access to the Archivist and will be devoted to policy development and implementation related to NARA's telework program.

Impact of Inconsistent and Inadequate Implementation of Telework Policy and Guidance

Effective performance management is recognized as a key component of a successful telework program. OPM guidance states management expectations for performance should be clearly addressed—and like non-teleworking employees—teleworkers should be held accountable for the results they produce. NARA's telework policy provides a number of tools to facilitate telework oversight and communication between the supervisor and teleworker. However, due to a lack of adequate training, guidance, and support, supervisors are not consistently implementing the telework program in accordance with policy and best practices. NA officials acknowledged further efforts need to be made to ensure NARA's telework program meets established requirements.

Further, although agencies are required to establish policy under which eligible employees may participate in telework to the maximum extent possible, this is dependent upon undiminished employee performance. OPM guidance states the manager must be kept apprised of the teleworker's schedule, how to make contact with the teleworker, and the status of all pending work. However, NARA telework managers have not consistently implemented the controls that facilitate communication and mitigate the inherent reduction in physical oversight and supervision associated with telework. Until NARA fully implements its telework program in accordance with the Telework Enhancement Act and best practices, it will not be able to ensure proper telework performance management.

Recommendations

2. We recommend the Chief Human Capital Officer (H):

    a. Develop training in accordance with the Telework Enhancement Act and OPM guidance to ensure agency wide understanding of the telework program and policy.
    b. Establish a process for sampling and reviewing telework forms for adequacy and accuracy.
    c. Publicize the name of the designated Telework Managing Officer and provide accurate contact information for future assistance.
    d. Ensure the revised telework policy is free of redundancies and conflicting requirements.
    e. Issue an annual notice reminding supervisors of their responsibilities regarding telework.

Management Response

Management concurred with the recommendations.

3. Security of NARA's Work-at-Home System is Vulnerable

Although NARA's Work-at-Home System (WAHS) was developed to enhance remote access security and provide enterprise-wide telework capabilities, the system remains vulnerable to the threats it was intended to mitigate. This condition exists because the WAHS was not fully developed, tested, or administered in accordance with NARA policy and Federal requirements. As a result, NARA's remote access system is at increased risk of security compromise and does not meet the security capabilities and requirements that justified the system's development.

NIST Special Publication 800-46, *Guide to Enterprise Telework and Remote Access Security*, identifies the increased risk involved in implementing a remote access system. Specifically, NIST SP 800-46 states remote access servers provide a way for external hosts to gain access to internal resources, so their security is particularly important. In addition to permitting unauthorized access to resources, a compromised server could be used to eavesdrop on remote access communications and manipulate them, as well as to provide a "jumping off" point for attacking other hosts within the organization. Further, NIST SP 800-46 states the nature of remote access technology generally places it at higher risk than similar technologies only accessed from inside the agency.

In order to address the increased risks of providing a remote access capability, risks must be properly identified and protected against. NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, states it is of paramount importance that responsible officials understand the risks and other factors that could adversely affect organizational operations and assets, individuals, other organizations, and the Nation. Officials must understand the current status of their security programs and the security controls planned or in place to protect their information and information systems in order to make informed judgments and investments that mitigate risks to an acceptable level. Further, NIST SP 800-53 creates a foundation for the development and assessment methods and procedures for determining security control effectiveness.

NARA policy incorporates many of the NIST standards and identifies a number of tools and procedures used to manage the security of its programs and systems. NARA 804, *Information Technology (IT) Systems Security*, identifies security risk assessments and the development of system security plans as two important activities used to ensure security measures are adequate. The risk assessment influences the development of the security controls for particular information systems and generates much of the information needed for the associated system security plans. System security plans provide an overview of the information security requirements and describe the security controls in place or planned for meeting those requirements.

In August 2008, NARA began the initial pilot phase of its current remote access capability, known as the Work-At-Home-System (WAHS). The WAHS was developed to support

NARANet users' ability to telework. The two fundamental business drivers for the WAHS involved emergency preparedness and the need to implement a more secure level of authentication. To address these business drivers, the WAHS incorporates two major components: 1) Citrix Access Suite and 2) RSA SecurID. The Citrix Access Suite provides application streaming capabilities to deliver the NARANet General Support System (GSS) to remote desktops and laptops. This component also provides application security and access control. The second component—the RSA SecurID—uses hardware tokens and an authentication server in providing two-factor authentication to NARA's Citrix, Virtual Private Network (VPN), and web-based e-mail capabilities.

In addition to the business drivers, NH—in drafting the WAHS proposal—identified a number of negative security implications if NARA did not adopt a new remote access approach. These implications included:

- NARA will be non-compliant with specific Office of Management and Budget (OMB) mandates and Homeland Security Presidential Directives (HSPD) related to identification and authentication procedures;
- NARA will not have an enterprise-level remote access solution in place for its Work-at-Home staff;
- NARA staff members will be unable to access NARA@work or shared drives on NARANet servers from remote locations;
- NARANet e-mail will remain vulnerable to network and hacker attacks; and
- NARA will not be able to protect Personally Identifiable Information (PII) and NARA proprietary information from being distributed or compromised over its network and e-mail system.

Our review of the WAHS security requirements, testing, and administration found—despite implementing the WAHS—many of the implications listed above remain. Specifically, NARA's electronic authentication process remains noncompliant with HSPD-12. Further, although the WAHS requirements state the enterprise-level system shall support up to 3,000 users in the full operating capability implementation, the WAHS is currently only licensed to allow concurrent remote usage of approximately 8 percent of that requirement. Additionally, NARA's web-based e-mail application remains vulnerable to the same network and hacker attacks present prior to the WAHS implementation. Lastly, NARA remains unable to protect PII and NARA proprietary information from remote download, printing, or distribution.

WAHS Security Requirements Development

In order to determine the early level of security control and requirements analysis that went into the development of the WAHS, we requested requirements documentation from the WAHS Project Manager and IT Security Staff (NHI). Within the scope of system security, we reviewed the following WAHS requirements documentation:

- Full Proposal of the Work at Home project,
- WAHS CONOPS and Initial Requirements Specification, and
- WAHS Design Specification.

In addition to the fundamental business drivers and implications described earlier, the WAHS Full Proposal provides an overall summary of the selected solution. A portion of this summary describes how the Citrix Access Suite will provide application security and access control, allowing fine levels of policy-based control over the actions users can take with such items as printing and e-mail attachments. However, during our review, while observing volunteer teleworkers working from their respective alternative worksites, we discovered NARA employees still have the ability to print sensitive information (including PII) using the Citrix application. This came as a surprise to NH officials—therefore, one NH official confirmed the ability to print while working from home. However, NH officials later stated "apparently, printing is suppose to be enabled per [the Deputy CIO] at his request." Therefore, although the WAHS proposal details the ability to control remote printing, this is not something NARA utilizes. Further, although the Citrix application prevents teleworkers from downloading e-mail attachments onto their personal computers, NARA has not disabled its Novell web-based e-mail application, which functions separately from Citrix and does not restrict downloads. Therefore, as observed during our site visits, teleworkers continue to download sensitive information onto their personal computers. When asked why NARA continues to allow use of the less secure Novell webmail application, NH officials initially stated they did not know, aside from "nobody really wanted to let it go." However, more recently, the same officials indicated discussions were made about keeping the webmail application available so in a surge condition, e-mail access would not be limited to the maximum number of concurrent users of the Citrix portal.

The second requirements document reviewed—CONOPS and Initial Requirements Specification—describes the intended remote user access functions, remote user access services, and IT infrastructure components of the WAHS. In addition, the document contains initial requirements of the system. A selection of these requirements—as they relate to policy, standards, scope, function, and security of the WAHS—include:

- The system *shall* provide two-factor authentication capabilities,
- The system *shall* comply with all NARA Enterprise Architecture standards and guidelines,
- The system *shall* implement all applicable IT security controls as specified in the IT Security Architecture,

- The system *shall* complete all security certification and accreditation tasks prior to Initial Operating Capability (IOC) and Full Operating Capability (FOC), and
- The system *shall* support up to 3,000 users in the FOC implementation.

OMB Memorandum M-06-16, "Protection of Sensitive Agency Information" requires agencies to allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access. The WAHS utilizes passwords and Personal Identification Numbers (PINs) as one of the two-factors. The second factor—a device separate from the computer gaining access—is met by employing RSA hardware tokens. However, due to a recent sophisticated security breach that took place at the company that produces the RSA tokens used by NARA, an NH official acknowledged the RSA token no longer appears to be an effective component of a two-factor mechanism.

By no longer having a secure second factor, NARA is in effect relying on usernames and passwords to control remote access to the network. NH officials have indicated that NARA's remote access system is still secure because in addition to using the RSA token and PIN, NH never removed the Novell username and password access requirement. However, requiring a user to enter multiple passwords instead of only one does not compensate for an ineffective token device. User known passwords are vulnerable to—among other things—social engineering, shoulder surfing, and keylogging. In terms of keylogging and other malware, the WAHS was developed to allow access from any computer with an internet connection—whether that is a user's personal computer, the computer in a hotel lobby, or a computer at a public library—therefore, NARA has no control over the malware installed on the computers used in remotely accessing the network. An effective token generated access code mitigates these risks; however, user known passwords and PINs alone remain vulnerable.

In terms of complying with NARA Enterprise Architecture standards, *NARA IT Security Requirements* state the NARANet GSS shall provide multifactor access control as a common control for remote and local access to the network. Further, the multifactor access mechanisms shall include credentials from HSPD-12 compliant Personal Identity Verification (PIV) cards. The WAHS CONOPS (dated February 28, 2008) state the RSA SecurID tokens are an "interim solution" until NARA is able to implement PIV remote access authentication. Although HSPD-12 had established the requirement in 2004, when asked when this upgrade was expected to take place, an NH official stated it would be delayed until OMB "[tells] us to implement it whether we like it or not" and sets a final deadline. OMB Memorandum 11-11 "Continued Implementation of Homeland Security Presidential Directive (HSPD) 12—Policy for Common Identification Standard for Federal Employees and Contractors," dated February 3, 2011, establishes this deadline as October 1, 2011.

In addition, Enterprise Architecture *IT Security Policies* identify a number of NARA IT security objectives that apply to the WAHS. In particular, NARA must ensure that managers and users of NARA information systems are made aware of the security risks associated with their activities.

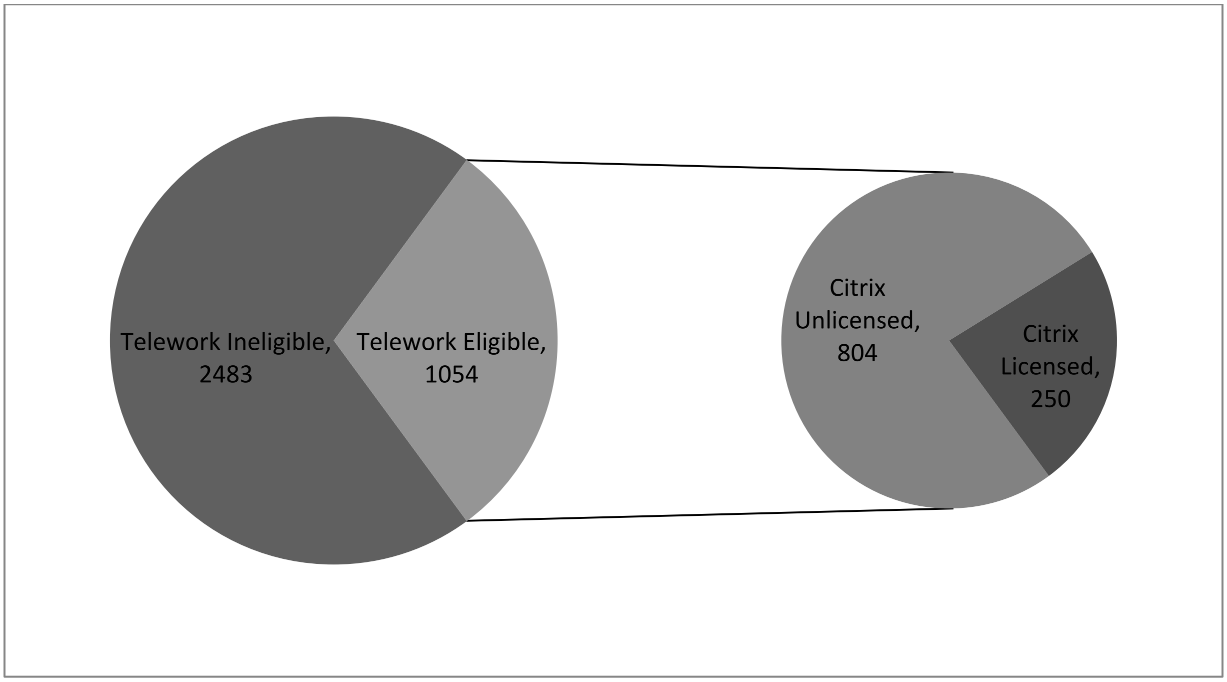
Further, NARA must ensure that personnel are adequately trained to carry out their assigned information security-related duties and responsibilities. NH officials indicated that other than a handout included with the distributed RSA tokens, no remote access IT security training has been developed or provided to teleworkers or their supervisors.

WAHS Project Management personnel were unable to provide exact dates of IOC or FOC; however, based on NARA Notices, the fully operational system was deployed in September 2009. Further, Project Management and NH personnel were unable to provide certification and accreditation documentation specific to the WAHS. The April 8, 2010 System Security Plan (SSP) for Network Infrastructure—which NH officials stated encompasses the WAHS—indicates that several components of the Network Infrastructure have already been certified and accredited as independent systems; however, the WAHS is not included in the list. Further, all mention of the WAHS in the SSP states the project is still under development, despite the WAHS reaching FOC seven months before the SSP update.

The Initial Requirements Specification indicates the WAHS will support up to 3,000 users. Both NA officials and NH officials stated the telework program and the supporting WAHS were developed independently from one another. This requirement reflects that lack of coordination, as according to the most recent data obtained from NA, the greatest number of employees actually teleworking in a given year since the program's inception was 334. Further, NH officials determined the greatest number of concurrent users was only 115. According to NH officials, NARA is currently licensed to accommodate 250 simultaneous users. Although this more precisely reflects actual usage, the WAHS must be able to support NARA's telework program once it is fully compliant with the Telework Enhancement Act.

In their recently updated Dismissal and Closure Procedures—with the advent of "unscheduled telework"—OPM states agencies should ensure IT infrastructure is in place to allow large numbers of employees to telework simultaneously. NH officials stated there is a point in which a high volume of concurrent usage would result in a degradation of WAHS performance, but NH has yet to determine actual system capacity. The chart below depicts the most recent tabulation of telework eligible employees in comparison to the number of Citrix Application simultaneous user licenses (see Chart 1 below). The number of eligible telework staff will likely increase once NARA fully conforms to Federal telework mandates.

Chart 1: Telework Eligible Staff in Relation to Citrix Users Licensed



The third requirements document reviewed—the WAHS Design Specification—details the design of the WAHS. The information contained in the document reflects the requirements and restraints of the CONOPS mentioned previously. Further, the Design Specification document includes a list of "to-be-determined (TBD) items." The list was used to identify and track all TBD items uncovered during the development of the WAHS. The document states all open questions and issues should be identified, documented, and tracked to completion within the WAHS Design Specification Appendix. The version dated April 23, 2008 contained 32 TBD items in the "open" status. Many of these open items related to system security. WAHS management personnel were unable to provide updates to the Design Specification document indicating these items were ever closed.

Security Testing

NARA's Enterprise Architecture IT Security Requirements contain security assessment requirements for the agency's IT programs. Specifically, the requirements state for all data, NHI shall develop a security assessment plan. Further, NHI is required to, at least annually, assess the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. NHI is required to produce a security assessment report that documents the results of the assessment.

NH personnel provided two documents that detailed security testing results, both of which took place prior to the WAHS entering production. These documents included: 1) Risk Assessment

Results, dated July 8, 2008 and 2) Security Assessment Plan and Procedures, also dated July 8, 2008. The Risk Assessment contained 16 different risk elements, ranging from unsuccessful login attempts to configuration change control. The assessment of nearly all risk elements indicated the WAHS was not in production and that it resided only in a test environment with no outside connections. As a result, the vast majority of the assessments concluded that the controls should be revisited once the system is in production. NH personnel were unable to provide definitive support that these controls were reassessed once the WAHS entered production.

As with the Risk Assessment, the Security Assessment Plan and Procedures report tested the requirements derived from NARA Security Architecture and NIST 800-53. A number of the requirements tested either failed or were deferred. Again, reasons for the deferred results were often explained by the WAHS not being in production at the time and that once in production, the controls would be implemented. However, NH personnel were unable to provide support that such actions actually took place. Further, NH personnel explained the WAHS is somewhat of anomaly, as most systems never have deferred testing[2]. NH personnel stated "a lot of people said we have to hurry up and test this thing, but a lot of the mechanisms weren't in place."

Further, some of the requirements tested during the Security Assessment were identified as passing, when current data indicates that they are not. Examples include patch management and auditable events. The flaw remediation category tested in the WAHS Security Assessment requires organizations to promptly install newly released security relevant patches. The results for this test indicated a pass rating, noting that patches will be installed once the system is transitioned into production. However, in a November 2010 NARA Information Security audit performed by GAO, the Citrix VPN server and client—key components of NARA's WAHS—were specifically identified as missing security patches. In addition, under the auditable events category tested in the WAHS Security Assessment, one of the associated requirements indicated that the information system generates audit records for events such as unsuccessful login attempts. Although the test results for this requirement indicated the Citrix Appliance passed, NH officials stated this capability only became available in March 2011—nearly three years after the testing took place.

WAHS Administration

In addition to assessing the documented security requirements and associated test plans, we also reviewed the ongoing administration of the WAHS as it relates to security control. NH personnel provided information and documentation that pertains to continuous efforts taken to ensure NARA's remote access system remains secure. Such procedures and documents are detailed below.

[2] NARA OIG Audit Report No. 09-15, "Audit of NARA's Work-at-Home System," dated September 29, 2009, identified concerns related to the WAHS not meeting OMB and NIST requirements prior to full implementation. Although management concurred with the recommendation to ensure requirements were met, WAHS documentation indicates a number of deferred and failed security testing at the time of implementation.

When discussing the identified issues in the requirements and test documentation, NH officials stated the WAHS security documentation has been superseded by the SSP. NH personnel indicated that the WAHS falls under the SSP for Network Infrastructure. Although the Network Infrastructure SSP is dated April 8, 2010, the plan has not been updated to reflect the WAHS. For example, the SSP states "currently, NARA employs a VPN solution that does not employ a two-factor authentication scheme." In addition, the SSP states "NARA currently has a project underway to develop a remote access capability to support users' ability to telework." However, according to NH officials, the WAHS was in full operation by September 2009, therefore, this should have been reflected in the April 2010 SSP. Further, although NH officials stated the SSP supersedes the earlier security documentation, the SSP specifically states "for more information on this solution, and a detailed discussion of the design and security mechanisms, please refer to the following documents," which include the WAHS CONOPS and Initial Requirements Specification, Work At Home Full Proposal, and WAHS Design Specification detailed earlier.

Shortly before the WAHS went into initial production, the WAHS Business Process Owner entered into a Service Level Agreement (SLA) with the Office of Information Technology Services Division (NHT). According to the August 4, 2008 SLA, in order to ensure the security of hosting platforms and operational infrastructure, certain activities (running scans, installing security patches, monitoring activity, etc.) were to be conducted prior to transitioning the WAHS to an operational state. As the service provider, NHT was responsible for performing these activities; however, NH officials stated many of these security activities were actually the responsibility of NHI.

In terms of installing security patches, NIST 800-46, *Guide to Enterprise Telework and Remote Access Security*, states it is particularly important for organizations to ensure that remote access servers are kept fully patched. However, as mentioned earlier, GAO identified key components of NARA's WAHS were missing security patches. NH officials stated patch management is an issue on all NARA servers and the issue is being addressed through their plan of action and milestones process.

In addition, the SLA states if there are any findings or security vulnerabilities discovered on the WAHS after it has been placed in an operational state, NH will take immediate steps to secure the platform. One vulnerability impacting the WAHS—which was mentioned previously—is the RSA token breach. When the breach became known, US CERT issued required mitigation procedures to agencies employing RSA tokens. Although these mitigation procedures were identified in March 2011, some have yet to be implemented at NARA. These include requiring [redacted] NH indicated that the impact of these changes are still under review by the CISO and are not yet implemented. NH officials stated they are waiting to see how events progress. However, during this time the network of a major military contractor that also uses the RSA token was hacked. The network compromise occurred despite the addition of a secondary password to its remote log-in process.

NH officials informed US CERT that one of the mitigation efforts NARA has undertaken to address the RSA vulnerability is to enable extensive logging. Specifically, this includes extensive logging for all enterprise authentication servers and collection of IP addresses of the system accessing the service, the username, the resource accessed, and whether the attempt was successful or not. However, when log reports were requested, NH officials indicated the log capability for Citrix logging server has a "broken" password. The NH official stated they "believe the logs are there, we just don't have access to log into the server." This has been the situation since at least the beginning of May 2011. NH officials did, however, provide logs generated by the RSA authentication server, although these did not [redacted]. Further, the RSA authentication is only one component of the process. If the RSA authentication is compromised, NH officials indicated they [redacted].

Further, while other RSA clients are urgently lining up to replace their compromised tokens, in response to the Committee on National Security Systems, NH officials stated NARA did not need to be on the priority list. NH officials indicated there was less urgency because NARA—like the hacked military contractor mentioned earlier—has an additional password credential in place. Additionally, NH officials indicated a plan is in place at NARA to deploy an alternative. NH officials stated they will be deploying the infrastructure to support the HSPD-12 compliant PIV card in less than six months, by the mandatory October 1, 2011 deadline. However, NH officials stated an enterprise-wide capability is dependent upon the acquisition of card readers and middleware, which reflect a significant life-cycle cost.

Impact of WAHS Vulnerabilities

NIST recognizes that remote access servers provide a way for external hosts to gain access to internal resources; therefore, their security is particularly important. However, despite the added risk associated with remote access, NARA did not thoroughly develop and test the WAHS in accordance with security policy. The WAHS was rushed through security assessment testing by deferring many key security tests. Once the system went into production, there is little evidence the deferred testing was ever reassessed. NH officials stated the remote access security is encompassed within the SSP, however, the plan does not reflect the remote access controls and system currently in place. Now that the system is fully operational, identified vulnerabilities remain unmitigated and inadequate responses to new threats leaves the WAHS susceptible to compromise.

Recommendations

3. We recommend the Executive for Information Systems and Chief Information Officer (I) and the Executive for Business Support Services (B):

a. Ensure all deferred and failed security tests have been reassessed and the results documented.
b. Update SSP to reflect NARA's remote access system.
c. Ensure all RSA breach mitigating procedures reported to US CERT are implemented and functioning.
d. Monitor compliance with HSPD-12 to ensure established deadlines are met.
e. Review Citrix security configurations for adequacy.
f. Ensure WAHS patches are current and monitored.
g. Develop a plan with General Counsel (NGC) to protect PII and NARA proprietary information from being distributed or compromised over the network and e-mail system.
h. Establish a cross functional team with the Office of Human Capital (H) to ensure remote access capabilities will meet increased NARA telework demands and to ensure appropriate security guidance is included in NARA telework policy.

Management Response

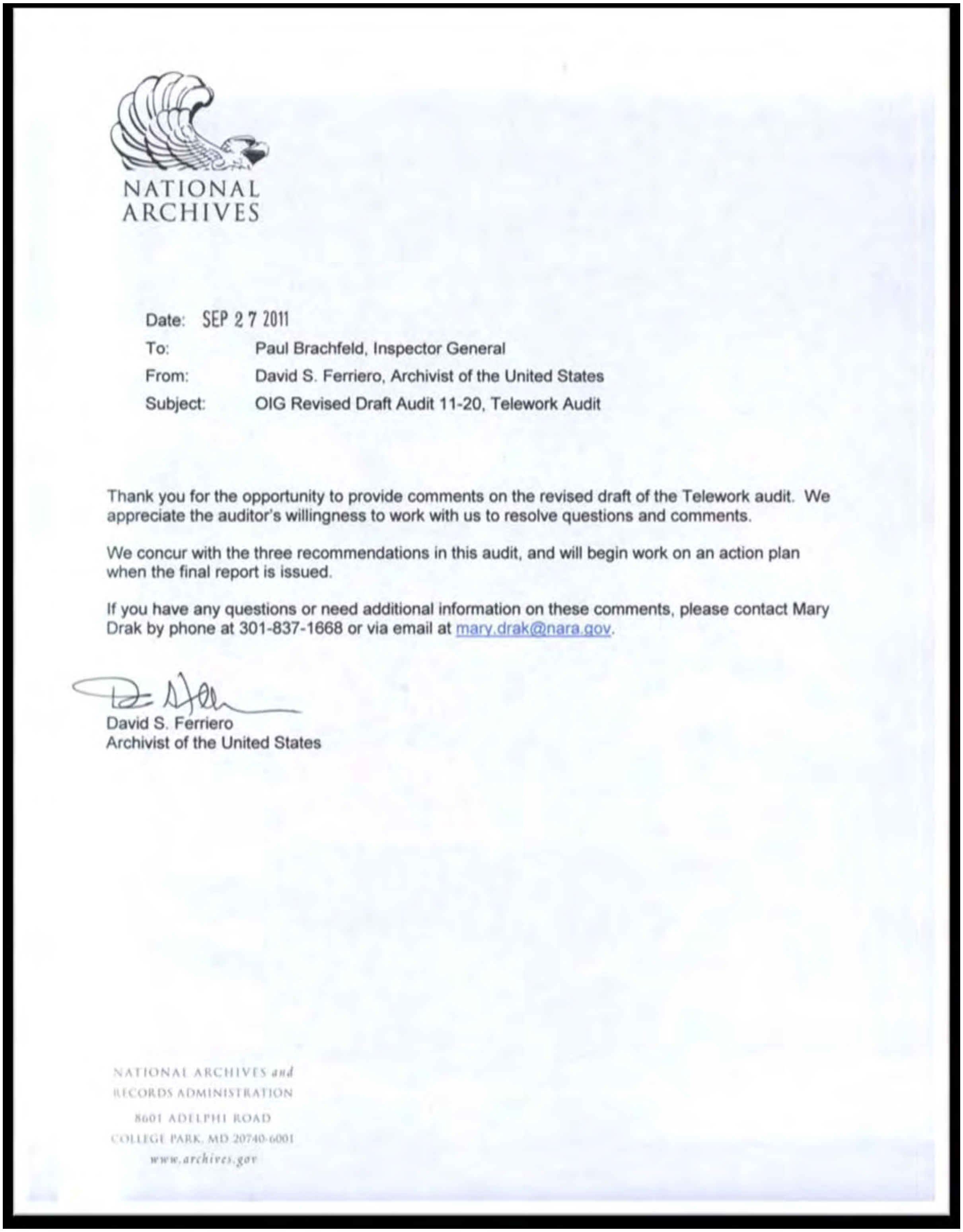
Management concurred with the recommendations.

Appendix A – GAO Key Telework Practices for Implementation of Successful Federal Telework Programs

Program planning • Designate a telework coordinator. • Establish a cross-functional project team, including, for example, information technology (IT), union representatives, and other stakeholders. • Establish measurable telework program goals. • Develop an implementation plan for the telework program. • Develop a business case for implementing a telework program. • Provide funding to meet the needs of the telework program. • Establish a pilot program.
Telework policy • Establish an agency-wide telework policy. • Establish eligibility criteria to ensure that teleworkers are selected on an equitable basis using criteria such as suitability of tasks and employee performance. • Establish policies or requirements to facilitate communication among teleworkers, managers, and coworkers. • Develop a telework agreement for use between teleworkers and their managers. • Develop guidelines on workplace health and safety issues to ensure that teleworkers have safe and adequate places to work off-site.
Performance management • Ensure that the same performance standards, derived from a modern, effective, credible, and validated performance system, are used to evaluate both teleworkers and non-teleworkers. • Establish guidelines to minimize adverse impact on non-teleworkers before employees begin to work at alternate worksites.
Managerial support • Obtain support from top management for a telework program. • Address managerial resistance to telework.
Training and publicizing • Train all involved, including, at a minimum, managers and teleworkers. • Inform workforce about the telework program.
Technology • Conduct assessment of teleworker and organization technology needs. • Develop guidelines about whether organization or employee will provide necessary technology, equipment, and supplies for telework. • Provide technical support for teleworkers. • Address access and security issues related to telework. • Establish standards for equipment in the telework environment.
Program evaluation • Establish processes, procedures, and/or a tracking system to collect data to evaluate the telework program. • Identify problems and/or issues with the telework program and make appropriate adjustments.

Source: GAO analysis of telework-related literature and guidelines.

Appendix B – Management's Response to the Report



NATIONAL
ARCHIVES

Date: SEP 2 7 2011

To: Paul Brachfeld, Inspector General

From: David S. Ferriero, Archivist of the United States

Subject: OIG Revised Draft Audit 11-20, Telework Audit

Thank you for the opportunity to provide comments on the revised draft of the Telework audit. We appreciate the auditor's willingness to work with us to resolve questions and comments.

We concur with the three recommendations in this audit, and will begin work on an action plan when the final report is issued.

If you have any questions or need additional information on these comments, please contact Mary Drak by phone at 301-837-1668 or via email at mary.drak@nara.gov.

David S. Ferriero
Archivist of the United States

NATIONAL ARCHIVES and
RECORDS ADMINISTRATION
8601 ADELPHI ROAD
COLLEGE PARK, MD 20740-6001
www.archives.gov

Appendix C - Report Distribution List

Archivist of the United States (N)
Deputy Archivist of the United States (ND)
Chief Operating Officer (C)
Chief Human Capital Officer (H)
Executive for Information Services and Chief Information Officer (I)
Executive for Business Support Services (B)
Performance and Accountability Office (CP)