

Department of Homeland Security **Office of Inspector General**

DHS' System To Enable Telework Needs a Disaster Recovery Capability



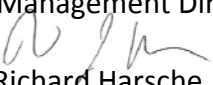


OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

March 21, 2014

MEMORANDUM FOR: Luke J. McCormack
Chief Information Officer
Management Directorate

FROM: 
Richard Harsche
Acting Assistant Inspector General
Office of Information Technology Audits

SUBJECT: *DHS' System To Enable Telework Needs a Disaster
Recovery Capability*

Attached for your information is our final letter report, *DHS' System To Enable Telework Needs a Disaster Recovery Capability*. We incorporated the formal comments from the Management Directorate in the final report.

The report contains two recommendations aimed at improving the Workplace as a Service. Your office concurred with both recommendations. As prescribed by *Department of Homeland Security Directive 077-01, Follow-Up and Resolution for Office of Inspector General Report Recommendations*, within 90 days of the date of this memorandum, please provide our office with a written response that includes your (1) agreement or disagreement, (2) corrective action plan, and (3) target completion date for each recommendation. Also, please include responsible parties and any other supporting documentation necessary to inform us about the current status of the recommendations.

Once your office has fully implemented the recommendations, please submit a formal closeout request to us within 30 days so that we may close the recommendations. The request should be accompanied by evidence of completion of agreed-upon corrective actions.

Please email a signed PDF copy of all responses and closeout requests to OIGITAuditsFollowup@oig.dhs.gov. Until your response is received and evaluated, the recommendations will be considered open and unresolved.

Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our report to appropriate congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the final report on our website for public dissemination.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Major contributors to this report are Sharon Huiswoud, Director; Kevin Burke, Supervisory Auditor; Charles Twitty, Senior Auditor; and Steven Tseng, IT Specialist.

Please call me with any questions, or your staff may contact Sharon Huiswoud, Director, Information Systems Division, (202) 254 5451.

Attachment



Background

The *Telework Enhancement Act of 2010*, Public Law 111-292, was enacted on December 9, 2010, to improve telework across the Federal Government. Additionally, on July 15, 2011, the Office of Management and Budget (OMB) issued a memorandum highlighting the benefits of teleworking, citing increases in productivity and reduced overhead costs. OMB has also emphasized the need for safeguards and reminded Federal agencies that, if not properly implemented, telework might introduce new security vulnerabilities into agency systems and networks.

The Office of the Chief Information Officer (OCIO) is implementing two systems to enhance telework in the Department of Homeland Security (DHS). These systems are called Workplace as a Service (WPaaS) and are part of an overall effort to move to cloud-based services. In September 2011, DHS awarded within scope task order modifications to the contractors operating DHS' Data Center 1 (DC1) and Data Center 2 (DC2) to implement WPaaS. Under the task orders, the contractors were to provide the government with complete physical environments which would provide the same functionality available on current DHS laptops and desktops. In addition, the task orders required the contractors to make the respective workplace environments accessible from all DHS components and organizations and from anywhere within the DHS OneNet and through appropriate technologies from any location where employees conduct work.

The WPaaS systems provide a virtualized desktop on a remote server located at one of the DHS data centers. The contractors were to provide a user experience equivalent to that of the user's local Windows desktop. DHS components provide images to the data center contractors that are similar to what the component users have on their desktops. These images then form the basis for creating an individual user's virtual desktop. Individual user settings and customizations, such as desktop wallpaper, are applied to the virtual desktop from a WPaaS user profile management system.

For WPaaS, telework employees access their virtual desktop by starting a virtual private networking session and connecting through the WPaaS Access Portal. The user credentials are authenticated against the DHS authentication system and then passed to the WPaaS servers to initiate a virtual desktop session. The contractor provides WPaaS storage space for the virtual desktops through a storage area network located at each data center.

The contractors have installed hardware, software, and telecommunications capabilities at DC1 and DC2 to implement WPaaS. Under the task orders, the contractor bears the costs to set up, manage, and deliver WPaaS. Subsequently, after OCIO places WPaaS in a



production environment, OCIO will charge the components for specific WPaaS capabilities. Specifically, DHS will reimburse the contractors based on the costs associated with WPaaS contract line item numbers (CLIN). The OCIO developed these CLINs to cover the contractors' costs for providing WPaaS services, plus a margin for fees.

Additionally, OCIO has provided funding to the components for WPaaS user testing.¹ The contractors have created WPaaS user IDs and virtual desktop images for approximately 750 users from DHS components. These users have tested the ability of the DC1 WPaaS system to access their component's information systems.

DHS requires both WPaaS contractors to provide continuity of operations and disaster recovery capabilities.

Results of Audit

DHS' System To Enable Telework Needs a Disaster Recovery Capability

DHS OCIO needs to ensure the Department's initiative to enhance telework, WPaaS, has a disaster recovery capability, including an alternate processing site. Without an alternate processing site, DHS employees who use WPaaS to telework would not be able to access their systems and data during an emergency situation. For example, if there were an outage at DC1, WPaaS users would have to wait for DC1 to be restored before they could once again access their systems.

Initially, the contractors were to implement a WPaaS system at each of DHS' data centers, DC1 and DC2. However, the different WPaaS versions developed by the respective DC1 and DC2 contractors did not provide alternate processing capabilities for each other. According to DHS staff, each contractor would need to establish a WPaaS space at the other contractor's data center to enable an alternate processing site. However, the contractors have not implemented the required alternate processing capability. Additionally, a WPaaS contractor space at the other contractor's facility has not been established because no DHS component has agreed to purchase contingency processing capability.

Further, in June 2013, OCIO decided to discontinue funding for WPaaS at DC2 due to delays stemming from technical issues that developed as the contractor was attempting to implement WPaaS at DC2. According to OCIO, the DC2 contractor did not provide a

¹ According to the Department, \$2,627,561.27 was obligated to enable components to use WPaaS.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

working solution to meet the minimum requirements, and in June 2013, OCIO postponed implementing WPaaS at DC2.

According to the Department's FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* review, the DC1 WPaaS has a security categorization of moderate. According to the National Institute of Standards and Technology (NIST), for all moderate- or high-impact systems, the contingency plan should include a strategy to recover and perform system operations at an alternate facility for an extended period.² In addition, NIST 800-34 recommends that contingency planning controls for systems with a moderate security categorization should include the identification of an alternate processing site. Further, NIST also recommends that the organization should identify an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.³

OCIO has recognized contingency planning deficiencies in the security plan for the DC1 WPaaS, including both the need for an alternate processing site and the need for plans to recover operations at an alternate site. OCIO designated these deficiencies as a moderate risk, and has left it up to the components using WPaaS to determine whether an alternate processing site is needed for their particular situations. If a component determines it needs an alternate site for WPaaS, the WPaaS contractor can provide a cost estimate for this capability. As of November 2013, no DHS component had committed to purchasing this capability.

We have identified the need for adequate contingency planning at DHS in previous reports. For example, in August 2013, we reported that DHS needed to update contingency plans to reflect current system information.⁴ Based on our review of plans for seven enterprise mission essential systems, we determined that two of seven plans did not identify adequate alternate locations for contingency operations.

² NIST Special Publication 800-34 Revision 1, *Contingency Planning Guide for Federal Information Systems*, May 2010.

³ NIST Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013.

⁴ *DHS Needs To Strengthen Information Technology Continuity and Contingency Planning Capabilities* (OIG-13-110), August 2013.



Recommendations

We recommend that the DHS Chief Information Officer (CIO):

Recommendation #1:

Identify an alternate processing site for the DC1 WPaaS.

Recommendation #2:

Revise the DC1 WPaaS contingency plan to include a strategy to recover and perform system operations at an alternate processing site for an extended period.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the Director, Departmental GAO-OIG Audit Liaison Office. We have included a copy of the comments in their entirety at appendix B. DHS concurred with recommendations one and two. Additionally, Management Directorate provided a summary of the actions they plan to take to implement these recommendations. Until we receive the corrective action plan with target completion dates and supporting documentation for the implementation of their actions, we consider recommendations 1 and 2 open and unresolved.



Appendix A

Objectives, Scope and Methodology

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the Department.

One of the objectives of this audit was to determine whether the OCIO had implemented required security documentation for the WPaaS, including effective disaster recovery plans. Due to the WPaaS objectives to enhance telework capability, we determined the OCIO's WPaaS systems to be within our audit scope.

We conducted the audit primarily in the Washington, DC area, as well as at DC1 and DC2. We reviewed WPaaS associated documentation such as the authority-to-operate letters, vulnerability assessments, contingency plans, and requisitions. We also reviewed applicable DHS and component policies and procedures, as well as government-wide guidance. We gave briefings and presentations to DHS staff concerning the results of fieldwork and the information summarized in this report.

We conducted this performance audit between March 2013 and November 2013 pursuant to the *Inspector General Act of 1978*, as amended, and according to 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 upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix B
Management Comments to the Draft Letter Report

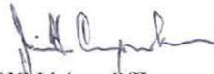
U.S. Department of Homeland Security
Washington, DC 20528



Homeland
Security

February 28, 2014

MEMORANDUM FOR: Richard Harsche
Acting Assistant Inspector General
Office of Information Technology Audits

FROM: Jim H. Crumpacker 
Director
Departmental GAO-OIG Liaison Office

SUBJECT: OIG Draft Report: "DHS' Initiative to Enhance Telework Needs a
Disaster Recovery Capability" (Project No. 13-006-ITA-MGMT)

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the Office of Inspector General's (OIG's) work in planning and conducting its review and issuing this report.

DHS is pleased to note OIG's recognition that the DHS Office of the Chief Information Officer (OCIO) has developed a Work Place as a Service (WPaaS) offering that provides a virtual desktop with a user experience equivalent to that of the user's local Windows desktop. DHS OCIO's WPaaS can be used both for teleworking and as an alternative to the desktop workstation to reduce operational costs.

The draft report contained two recommendations with which the Department concurs. Specifically, OIG recommended that the DHS Chief Information Officer:

Recommendation 1: Identify an alternate processing site for the DC1 [Data Center 1] WPaaS.

Response: Concur. DHS OCIO has selected Data Center Two (DC2) as the alternate processing site for WPaaS and is documenting it as such in the appropriate security plans. If Components require an alternate processing site, they have the option to purchase the necessary Contract Line Item Numbers for services needed to meet their Component-specific requirements. This enables Components to make the best use of funding and most efficient use of resources to achieve their respective missions. Estimated Completion Date (ECD): April 30, 2014.

Recommendation 2: Revise the DC1 WPaaS contingency plan to include a strategy to recover and perform system operations at an alternate processing site for an extended period.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Response: Concur. DHS OCIO is revising the WPaaS contingency plan to include DC2 as the alternate site for system recovery and will also amend the appropriate security plans.
ECD: April 30, 2014.

Again, thank you for the opportunity to review and comment on this draft report. Technical comments were previously provided under separate cover. Please feel free to contact me should you have any questions. We look forward to working with you again in the future.



Appendix C

Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Under Secretary for Management
DHS CIO Audit Liaison
DHS Chief Information Security Officer
DHS CISO Audit Liaison
Chief Privacy Officer

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

ADDITIONAL INFORMATION

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General (OIG) Office of Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov, or follow us on Twitter at: [@dhsoig](https://twitter.com/dhsoig).”

OIG HOTLINE

To expedite the reporting of alleged fraud, waste, abuse or mismanagement, or any other kinds of criminal or noncriminal misconduct relative to Department of Homeland Security (DHS) programs and operations, please visit our website at www.oig.dhs.gov and click on the red tab titled "Hotline" to report. You will be directed to complete and submit an automated DHS OIG Investigative Referral Submission Form. Submission through our website ensures that your complaint will be promptly received and reviewed by DHS OIG.

Should you be unable to access our website, you may submit your complaint in writing to:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Office of Investigations Hotline
245 Murray Drive, SW
Washington, DC 20528-0305

You may also call 1(800) 323-8603 or fax the complaint directly to us at (202) 254-4297.

The OIG seeks to protect the identity of each writer and caller.