IMPLEMENTATION REVIEW OF ALERT REPORT ON SECURITY OF GSA'S ELECTRONIC MESSAGING SERVICES AND NATIONAL NOTES INFRASTRUCTURE
REPORT NUMBER A070180/O/T/W07001
DATED SEPTEMBER 12, 2007
ASSIGNMENT NUMBER A100099

March 31, 2010

U.S. GENERAL SERVICES ADMINISTRATION
Office of Inspector General

Date: March 31, 2010

Reply to Gwendolyn McGowan
Attn of: Deputy Assistant Inspector General for Information Technology Audits (JA-T)

Subject: Implementation Review of Alert Report on Security of GSA's Electronic Messaging Services and National Notes Infrastructure, Report Number A070180/O/T/W07001, dated September 12, 2007, Assignment Number A100099

To: Casey Coleman
Chief Information Officer, Office of the Chief Information Officer (I)

The Information Technology (IT) Audit Office has completed an implementation review of the management actions taken in response to the seven recommendations included in the subject audit report. This implementation review found that GSA has completed a majority of the steps identified in the action plan. As a result, security controls for GSA's Lotus Notes environment have been significantly strengthened. Appendix A provides a summary of the steps taken by GSA to strengthen security controls for the Agency's Lotus Notes environment, following our 2007 alert report, and instances where specific steps were not completed within the timeframe specified or were not yet finished. Specifically, related to our second recommendation to review and configure controls for all Lotus Notes databases and applications, we found that not all Lotus Notes servers were included in technical controls testing by the timeframe specified in the action plan. Further, two action steps for our third recommendation to identify and remove outdated Lotus Notes applications have not been completed at this time. These action steps were planned to: (1) purge and consolidate outdated Lotus Notes applications across GSA and (2) complete certification[1] and accreditation[2] (C&A) of GSA's Lotus Notes applications.

Background

In 2007, we reported that significant management, operational, and technical control weaknesses within GSA's Lotus Notes environment had put the security of essential information, equipment, services, and systems at undue risk. If exploited, these vulnerabilities could have impaired GSA's ability to carry out its mission. We also reported that risks for GSA's Lotus Notes environment had not been adequately considered under GSA's IT Security Program or through established system security C&A processes. On November 14, 2007, the GSA Office of the Chief Information Officer (OCIO) provided a formal, time-phased audit action plan that identified action steps that it had planned in response to our findings and recommendations

[1] Certification refers to the process utilized to determine the extent to which controls are implemented correctly and operating as intended.
[2] Accreditation is the official management decision to authorize operation of an information system and to explicitly accept the risk to agency operations, assets, or individuals based upon the implementation of controls.

related to Lotus Notes security controls. Since then, the OCIO has established a new governance structure for GSA's Lotus Notes environment. In May 2009, the action plan was revised to include additional steps aimed at addressing our recommendation to purge certain Lotus Notes databases, applications, and web pages as needed. Appendices B and C contain the original and revised action plans. Appendix D contains comments provided by you on our draft letter report.

Objective, Scope, and Methodology

The objective of this implementation review was to determine if the action steps were completed as stated in the action plan. We conducted this assessment in accordance with section 807.02, *Implementation Reviews*, of the GSA *Office of Inspector General Policy and Procedures Manual*. To accomplish our objective, we reviewed specific documentation that the OCIO developed in response to our audit. We also met with the OCIO Information System Security Manager, the Director of the Enterprise Applications and Services Committee, and IT officials within the Public Buildings Service (PBS) and Federal Acquisition Service (FAS) to gain an understanding of the actions taken to secure their respective Lotus Notes databases and applications. We conducted appropriate, limited testing to determine whether or not reported conditions have been corrected by the actions taken and to verify our results.

Results of Implementation Review

The OCIO has taken important steps to improve risk management practices for the Agency's Lotus Notes environment following our 2007 alert report. This review found that the majority of steps identified in the action plan for our alert report were completed as planned. However, we found that (1) technical controls testing was not performed for all Lotus Notes applications and databases within the timeframe specified in the action plan for our second recommendation; and (2) purging and consolidation activities and C&A of security controls for Lotus Notes applications and databases were not completed as stated in the action plan for our third recommendation. We recognize that completion of these activities is important as GSA considers utilizing cloud computing services for portions of its Lotus Notes infrastructure. To address the results for this implementation review, the OCIO should submit a revised action plan responding specifically to Recommendation #3 to GSA's Internal Control and Audit Division (BEI) within 30 days.

If you have any questions regarding this review, please contact Gwendolyn McGowan, Deputy Assistant Inspector General for Information Technology Audits, or me at 703-308-1223.

Khalid Hasan

Khalid Hasan
Audit Manager
Information Technology Audit Office (JA-T)

IMPLEMENTATION REVIEW OF ALERT REPORT ON
SECURITY OF GSA'S ELECTRONIC MESSAGING SERVICES
AND NATIONAL NOTES INFRASTRUCTURE
REPORT NUMBER A070180/O/T/W07001
DATED SEPTEMBER 12, 2007
ASSIGNMENT NUMBER A100099

APPENDIX A - SUMMARY STATUS OF ACTION STEPS IDENTIFIED IN THE GSA-CIO'S ACTION PLAN FOR THE OIG'S 2007 LOTUS NOTES ALERT REPORT

Recommendation From OIG Alert Report	Agency Action Step	Status of Action Step
1. Develop a complete inventory of GSA's Lotus Notes databases and applications.	• Run an agent on all Lotus servers monthly and record all nsf files (i.e. databases) in a Lotus database.	• The action step was completed as stated and the GSA-OCIO has developed an inventory that is updated on a monthly basis. The inventory does not include the types of information stored in Lotus Notes databases or applications.
2. Review and configure controls for all Lotus Notes databases, applications, and associated Intranet and Internet websites to ensure that appropriate access is granted.	• Run agent on all Lotus servers and record all nsf files (i.e. databases) that have default set to greater than No ACCESS and review and change as necessary.	• While the action step was completed as stated, it was completed past the planned timeframe. The OCIO has created a tool that periodically assesses access control settings for all Lotus Notes databases and applications across the Agency. These settings are then reviewed to ensure appropriate access is granted. The tool only assesses permissions granted to the "default" level.

Recommendation From OIG Alert Report	Agency Action Step	Status of Action Step
3. Identify and remove all Lotus Notes databases, applications, and Intranet and Internet web pages residing on GSA's Lotus Notes infrastructure that are outdated, lack necessary controls, or do not adhere to guidelines for GSA's websites, including those we have identified in Appendix B.	Note: In May 2009, the OCIO submitted a revised action plan for this recommendation, to complete a comprehensive restructuring of management of Lotus Notes databases. Revised Action Step: Inventory Notes and Domino databases and applications. Give to FAS and PBS those which are theirs.	• The action step was completed as stated. The GSA OCIO has developed an inventory of Notes and Domino databases and applications and a proposal to give FAS and PBS security management for their respective Lotus Notes applications and databases was approved in July 2008.
	Revised Action Step: Through the new IT governance structure, review the GM&A databases and applications, purging those no longer used, consolidating those performing similar functions, and establishing rules for creating new databases.	• This action step has not been completed as planned. Specifically, the OCIO has not completed the process of identifying and purging outdated databases and applications. • FAS and PBS officials estimated approximately 70% and 45% completion rates respectively for purging their outdated databases and applications.
	Revised Action Step: Perform a C&A on the GM&A Notes and Domino databases and applications; inventory applications on web servers and perform an Enterprise Applications C&A on all applications for which the OCIO is responsible.	• This action step has not been completed as planned. While the OCIO has completed a C&A for the Lotus Notes infrastructure, it has not finished performing a C&A for agencywide Notes applications. • FAS and PBS have not completed a C&A for the Lotus Notes applications under their management.

Recommendation From OIG Alert Report	Agency Action Step	Status of Action Step
4. Develop policy and procedures on use and maintenance of GSA's National Notes Infrastructure to address: • Roles and responsibilities for establishing and maintaining Lotus Notes databases, applications, and Intranet and Internet web pages. • Security configuration requirements and considerations for Lotus Notes servers, databases, and applications, to include access controls, system development, and configuration. • Appropriate use of Lotus Notes databases and applications. • System training for email users and application developers regarding security considerations for Lotus Notes email, databases and applications.	• Create Lotus Security Implementation Guide.	• This action step was completed as planned. The GSA OCIO developed a Lotus Notes security procedural guide covering the areas listed in the report recommendation; the guide was provided to Lotus Notes application developers; and a reference to the guide was incorporated in annual security awareness training.
5. Reevaluate established definitions for the Enterprise Infrastructure Operations to determine if the criticality and sensitivity of information managed through GEMS and GNNI warrant a separate certification and accreditation of unique risks and system security controls.	• A decision will be made by Director, EIO as to whether the Notes Infrastructure will be separated from the EIO C&A and have its own C&A performed or that the EIO C&A will be enhanced to further secure the notes infrastructure.	• This action step was completed as planned. GSA has compartmentalized its Lotus Notes infrastructure, with the OCIO, PBS, and FAS responsible for security management for specific components.

Recommendation From OIG Alert Report	Agency Action Step	Status of Action Step
6. Complete a comprehensive certification and accreditation process for GEMS and GNNI to ensure that the risks and necessary controls for GSA's Lotus Notes environment are adequately identified and documented, including verification of user requirements for e-mail security.	• Based on the decision made in recommendation 5 above, a C&A Team will be formed, comprised of an independent 3rd party group, GSA IT Security Personnel and Notes Infrastructure Management & Administrators to conduct a full C&A for the Notes Infrastructure or take the steps necessary to enhance the present EIO System	This action step was completed as stated. However, the C&A for the Lotus Notes infrastructure did not address media controls and physical and environmental controls for all locations. In addition, adequate details on security controls assessment procedures were not included in the C&A.
7. Take immediate steps to strengthen technical controls for GEMS and GNNI by: (a.) including all Lotus Notes databases and applications, including mail files, in periodic technical controls testing and evaluation processes; (b.) verifying the adequacy of controls for e-mail servers hosted for external customers; and (c.) reviewing all Lotus Notes based Intranet and public facing agency web sites to ensure that unauthorized individuals cannot modify the contents and information presented on the sites.	• Run agent weekly on all Lotus servers and record all nsf files (i.e. databases) that have default set to greater than NO ACCESS and then change and review, as necessary. • Run Operating System scan on EAC servers and remediate vulnerabilities. • Run database scanner on EAC servers and remediate vulnerabilities. • Run agent on EAC servers and record all nsf files (i.e. databases) that have default set to greater than NO ACCESS and then change and review as necessary. • Review all Internet and Intranet Lotus websites.	These actions steps were completed as stated.

IMPLEMENTATION REVIEW OF ALERT REPORT ON
SECURITY OF GSA'S ELECTRONIC MESSAGING SERVICES
AND NATIONAL NOTES INFRASTRUCTURE
REPORT NUMBER A070180/O/T/W07001
DATED SEPTEMBER 12, 2007
ASSIGNMENT NUMBER A100099

APPENDIX B - ACTION PLAN FOR THE ALERT REPORT ON SECURITY OF GSA'S ELECTRONIC MESSAGING SERVICES AND NATIONAL NOTES INFRASTRUCTURE, REPORT NUMBER A070180/O/T/W07001 DATED SEPTEMBER 12, 2007

GSA

GSA Office of the Chief Information Officer

NOV 14 2007

MEMORANDUM FOR GWENDOLYN A. MCGOWAN
DEPUTY ASSISTANT INSPECTOR GENERAL FOR
INFORMATION TECHNOLOGY AUDITS (JA-T)

FROM: CASEY COLEMAN (I)
CHIEF INFORMATION OFFICER

SUBJECT: Alert Report on Security of GSA's Electronic Messaging Services and National Notes Infrastructure
Report Number A070180/O/T/W07001

This is in response to the IG audit on the above subject.

As a result of our review of your findings and recommendations cited in the audit, we have prepared an Action Plan on the audit report recommendations for the Office of the CIO.

If you have any questions, please contact Mike Seckar, Acting Chief of Staff, on 202-208-5054.

Attachments

U.S. General Services Administration
1800 F Street, NW
Washington DC 20405-0002
www.gsa.gov

Action Plan

Designated Responding Official: Kurt Garbars
Contact Person: Kurt Garbars
Telephone Number: 202-208-7485
Date: October 24, 2007

Action Report Number and Title	Recommendation Number	Proposed Recommendation Completion Date
Security of GSA's Electronic Messaging Services and national Notes Infrastructure Report Number A070180/O/T/W07001	1	December 31. 2007

Recommendation:

To strengthen management, operational, and technical security control weaknesses and ensure that GSA continues to benefit from the information sharing capabilities of GEMS and GNNI, we recommend that the GSA-Chief Information Officer work closely with GSA Services/Staff Offices/Regions to:

Develop a complete inventory of GSA's Lotus Notes databases and applications.

Action to be Taken Step by Step	Supporting Documentation To be sent to BECA	Documentation Will be Sent Last Day of
1. Run an agent on all Lotus servers monthly and record all nsf files (i.e. databases) in a Lotus database.	An example screenshot of databases tracked and the actual path to the database.	December 31, 2007

Action Plan

Designated Responding Official: Kurt Garbars
Contact Person: Kurt Garbars
Telephone Number: 202-209-7485
Date: October 24, 2007

Action Report Number and Title	Recommendation Number	Proposed Recommendation Completion Date
Security of GSA's Electronic Messaging Services and national Notes Infrastructure Report Number A070180/O/T/W07001	2	December 31, 2007

Recommendation:

Review and configure controls for all Lotus Notes databases, applications, and associated Intranet and Internet websites to ensure that appropriate access is granted.

Action to be Taken Step by Step	Supporting Documentation To be sent to BECA	Documentation Will be Sent Last Day of
Run agent on all Lotus servers and record all nsf files (i.e. databases) that have default set to greater than No ACCESS and review and change as necessary.	Export of servers with numbers of databases that have been approved at a default access level of NO ACCESS in excel spreadsheet format.	December 31, 2007

Action Plan

Designated Responding Official: Barbara Scott
Contact Person: Tom Eaton
Telephone Number: 817-829-2390
Date: October 24, 2007

Action Report Number and Title	Recommendation Number	Proposed Recommendation Completion Date
Security of GSA's Electronic Messaging Services and national Notes Infrastructure Report Number A070180/O/T/W07001	3	September 30, 2008

Recommendation:

Identify and remove all Lotus Notes databases, applications, and Intranet and Internet web pages residing on GSA's Lotus Notes infrastructure that are outdated, lack necessary controls, or do not adhere to guidelines for GSA's websites, including those we have identified in Appendix B.

Action to be Taken Step by Step	Supporting Documentation To be sent to BECA	Documentation Will be Sent Last Day of
1. Review inventory of Lotus Notes databases, applications and Intranet and Internet web pages residing on Lotus Notes Infrastructure and remove those that are no longer being used or do not adhere to guidelines for GSA's websites.	Number of Notes databases, applications and web pages, by server that were removed.	September 30, 2008

3

Action Plan

Designated Responding Official: *Kurt Garbars*
Contact Person: *Kurt Garbars*
Telephone Number: *202-208-7485*
Date: *October 24, 2007*

Action Report Number and Title	Recommendation Number	Proposed Recommendation Completion Date
Security of GSA's Electronic Messaging Services and national Notes Infrastructure Report Number A070180/O/T/W07001	4	June 30, 2008

Recommendation:

Develop policy and procedures on use and maintenance of GSA's National Notes Infrastructure to address:

1. Roles and responsibilities for establishing and maintaining Lotus Notes databases, applications, and Internet and Internet web pages.

Action to be Taken Step by Step	Supporting Documentation To be sent to BECA	Documentation Will be Sent Last Day of
1. Create Lotus Security Implementation Guide	Lotus Security Implementation Guide	November 30, 2007

4

Action Plan

Designated Responding Official: Kurt Garbars
Contact Person: Kurt Garbars
Telephone Number: 202-208-7485
Date: October 24, 2007

Action Report Number and Title	Recommendation Number	Proposed Recommendation Completion Date
Security of GSA's Electronic Messaging Services and national Notes Infrastructure Report Number A070180/O/T/W07001	4	June 30, 2008

Recommendation:

Develop policy and procedures on use and maintenance of GSA's National Notes Infrastructure to address:

2. Security configuration requirements and considerations for Lotus Notes servers, databases, and applications, to include access controls, system development, and configuration.

Action to be Taken Step by Step	Supporting Documentation To be sent to BECA	Documentation Will be Sent Last Day of
2. Create Lotus Security Implementation Guide	Lotus Security Implementation Guide	November 30, 2007

5

Action Plan

Designated Responding Official: Kurt Garbars
Contact Person: Kurt Garbars
Telephone Number: 202-208-7485
Date: October 24, 2007

Action Report Number and Title	Recommendation Number	Proposed Recommendation Completion Date
Security of GSA's Electronic Messaging Services and national Notes Infrastructure Report Number A070180/O/T/W07001	4	June 30, 2008

Recommendation:

Develop policy and procedures on use and maintenance of GSA's National Notes Infrastructure to address:

3. Appropriate use of Lotus Notes databases and applications.

Action to be Taken Step by Step	Supporting Documentation To be sent to BECA	Documentation Will be Sent Last Day of
3. Create Lotus Security Implementation Guide	Lotus Security Implementation Guide	November 30, 23007

6

Action Plan

Designated Responding Official: Kurt Garbars
Contact Person: Kurt Garbars
Telephone Number: 202-208-7485
Date: October 24, 2007

Action Report Number and Title	Recommendation Number	Proposed Recommendation Completion Date
Security of GSA's Electronic Messaging Services and national Notes Infrastructure Report Number A070180/O/T/W07001	4	June 30, 2008

Recommendation:

Develop policy and procedures on use and maintenance of GSA's National Notes Infrastructure to address:

4. System training for e-mail uses and application developers regarding security considerations for Lotus Notes e-mail, databases and applications.

Action to be Taken Step by Step	Supporting Documentation To be sent to BECA	Documentation Will be Sent Last Day of
1. Send application developers Lotus Security Implementation Guide for them to read	Email sent to developers	January 31, 2008
2. Incorporate Lotus Notes email security training in security awareness training.	Copy of awareness training content	June 30, 2008

7

Action Plan

Designated Responding Official: Phillip Klokis
Contact Person: Thomas M. Eaton
Telephone Number: 817-829-2390
Date: October 24, 2007

Action Report Number and Title	Recommendation Number	Proposed Recommendation Completion Date
Security of GSA's Electronic Messaging Services and national Notes Infrastructure Report Number A070180/O/T/W07001	5	January 31, 2008

Recommendation:

Reevaluate established definitions for the Enterprise Infrastructure Operations to determine if the critically and sensitivity of information managed through GEMS and GNNI warrant a separate certification and accreditation of unique risks and system security controls.

Action to be Taken Step by Step	Supporting Documentation To be sent to BECA	Documentation Will be Sent Last Day of
1. A decision will be made by Director, EIO as to whether the Notes Infrastructure will be separated from the EIO C&A and have its own C&A performed or that the EIO C&A will be enhanced to further secure the notes Infrastructure	Decision paper sent to Authorizing Official	January 31, 2008

8

Action Plan

Designated Responding Official: Phillip Klokis
Contact Person: Thomas M. Eaton
Telephone Number: 817-829-2390
Date: October 24, 2007

Action Report Number and Title	Recommendation Number	Proposed Recommendation Completion Date
Security of GSA's Electronic Messaging Services and national Notes Infrastructure Report Number A070180/O/T/W07001	6	

Recommendation:

Complete a comprehensive certification and accreditation process for GEMS and GNNI to ensure that the risks and necessary controls for GSA's Lotus Notes environment are adequately identified and documented, including verification of user requirements for e-mail security.

Action to be Taken Step by Step	Supporting Documentation To be sent to BECA	Documentation Will be Sent Last Day of
Based on the decision made in recommendation 5 above, a C&A Team will be formed, comprised of an independent 3rd party group, GSA IT Security Personnel and Notes Infrastructure Management & Administrators to conduct a full C&A for the Notes Infrastructure or take the steps necessary to enhance the present EIO System Security Plan.	A reaccredidation package for the EIO or a new C&A package for the Notes Infrastructure will be sent to the Authorizing Official to generate an Authority to Operate (ATO) memorandum	September 30, 2008

9

Action Plan

Designated Responding Official: Kurt Garbars
Contact Person: Kurt Garbars
Telephone Number: 202-208-7485
Date: October 24, 2007

Action Report Number and Title	Recommendation Number	Proposed Recommendation Completion Date
Security of GSA's Electronic Messaging Services and national Notes Infrastructure Report Number A070180/O/T/W07001	7	January 31, 2008

Recommendation:

Take immediate steps to strengthen technical controls for GEMS and GNNI by:

1. Including all Lotus Notes databases and applications, including mail files, in periodic technical controls testing and evaluation processes.

Action to be Taken Step by Step	Supporting Documentation To be sent to BECA	Documentation Will be Sent Last Day of
1. Run agent weekly on all Lotus servers and record all nsf files (i.e. databases) that have default set to greater than NO ACCESS and then change and review, as necessary.	Export of servers with numbers of databases that have been approved at a default access level of NO ACCESS in excel spreadsheet format.	December 31, 2007
2. Run quarterly scans on Lotus servers	Example copy of Foundstone report	December 31, 2007

10

Action Plan

Designated Responding Official: Kurt Garbars
Contact Person: Kurt Garbars
Telephone Number: 202-208-7485
Date: October 24, 2007

Action Report Number and Title	Recommendation Number	Proposed Recommendation Completion Date
Security of GSA's Electronic Messaging Services and national Notes Infrastructure Report Number A070180/O/T/W07001	7	January 31, 2008

Recommendation:

Take immediate steps to strengthen technical controls for GEMS and GNNI by:

2. Verifying the adequacy of controls for e-mail servers hosted for external customers.

Action to be Taken Step by Step	Supporting Documentation To be sent to BECA	Documentation Will be Sent Last Day of
1. Run Operating System scan on EAC servers and remediate vulnerabilities	Foundstone scan report	November 30, 2007
2. Run database scanner on EAC servers and remediate vulnerabilities	App detective scan report	December 31, 2007
3. Run agent on EAC servers and record all nsf files (i.e. databases) that have default set to greater than NO ACCESS and then change and review as necessary.	Export of servers with numbers of databases that have been approved at a default access level of NO ACCESS in excel spreadsheet format.	January 31, 2008

11

Action Plan

Designated Responding Official: Kurt Garbars
Contact Person: Kurt Garbars
Telephone Number: 202-208-7485
Date: October 24, 2007

Action Report Number and Title	Recommendation Number	Proposed Recommendation Completion Date
Security of GSA's Electronic Messaging Services and national Notes Infrastructure Report Number A070180/O/T/W07001	7	January 31, 2008

Recommendation:

Develop policy and procedures on use and maintenance of GSA's National Notes Infrastructure to address:

3. Reviewing all Lotus Notes based Intranet and public facing agency web sites to ensure that unauthorized individuals cannot modify the contents and information presented on the sites.

Action to be Taken Step by Step	Supporting Documentation To be sent to BECA	Documentation Will be Sent Last Day of
1. Review all Internet and Intranet Lotus websites	Copy of spreadsheets of IPs reviewed and brief summary of results	December 31, 2007

12

IMPLEMENTATION REVIEW OF ALERT REPORT ON
SECURITY OF GSA'S ELECTRONIC MESSAGING SERVICES
AND NATIONAL NOTES INFRASTRUCTURE
REPORT NUMBER A070180/O/T/W07001
DATED SEPTEMBER 12, 2007
ASSIGNMENT NUMBER A100099

APPENDIX C - REVISED ACTION PLAN FOR THE ALERT REPORT ON SECURITY OF GSA'S ELECTRONIC MESSAGING SERVICES AND NATIONAL NOTES INFRASTRUCTURE, REPORT NUMBER A070180/O/T/W07001, DATED SEPTEMBER 12, 2007

GSA

GSA Office of the Chief Information Officer

May 6, 2009

MEMORANDUM FOR RALPH L. BOLDT
DIRECTOR, INTERNAL CONTROL AND AUDIT
DIVISION (BEI)

FROM: CASEY COLEMAN
CHIEF INFORMATION OFFICER (I)

SUBJECT: Alert Report on Security of GSA's Electronic Messaging Services and National Notes Infrastructure
Report Number A070180/O/T/W07001

Attached for your review and action is a revised Action Plan for the following recommendation on Audit Report: Alert Report on Security of GSA's Electronic Messaging Services and National Notes Infrastructure.

The justification for the revised Action Plan and revised date is to complete a comprehensive restructuring of management of Notes and Domino databases.

Recommendation 3, Action Item 1

Please forward the revised Action Plan to the Inspector General.

If you have any questions, or if you need any additional information regarding this matter, please contact Dennis Papula, Director, Office of IT Policy and Compliance Division on 202-219-0180.

Attachments

U.S. General Services Administration
1800 F Street, NW
Washington, DC 20405-0002
www.gsa.gov

Revised
Action Plan

Designated Responding Official: Teresa Sorrenti
Contact Person: Barbara Scott
Telephone Number: 202-501-2375
Date: April 16, 2009

Action Report Number and Title	Recommendation Number	Proposed Recommendation Completion Date
Security of GSA's Electronic Messaging Services and national Notes Infrastructure Report Number A070180/O/T/W07001	3	**Revised June 30, 2009**

Recommendation:
To strengthen management, operational, and technical security control weakness and ensure that GSA continues to benefit from the information sharing capabilities of GEMS and GNNi, we recommend that the GSA-CIO work closely with Services/Staff Offices/Regions to identify and remove all Lotus Notes databases, applications, and Intranet and Internet web pages residing on GSA's Lotus Notes, infrastructure that are outdated, lack necessary controls, or do not adhere to guidelines for GSA's websites, including those we have identified in Appendix B.

Action to be Taken Step by Step	Supporting Documentation To be sent to BECA	Documentation Will be Sent Last Day of
1. Inventory Notes and Domino databases and applications. Give to FAS and PBS those which are theirs. 2. Through the new IT governance structure, review the GM&A databases and applications, purging those no longer used, consolidating those performing similar functions, and establishing rules for creation of new Domino databases. 3. Perform a C&A the GM&A Notes and Domino databases and applications. 4, Inventory applications on web servers and perform an Enterprise Applications C&A on all applications for which the OCIO is responsible.	Copy of Enterprise Communications Services C&A. (contains Notes and Domino applications) Copy of the Enterprise Applications C&A. (contains web services applications). Copy of IT Applications and Services Committee Charter. Summary of actions completed including excerpts from the Enterprise Applications and Services Committee minutes.	REVISED June 2009

JUSTIFICATION:

OCIO is taking actions to address the underlying issues relating to the recommendation. The end result will be a reorganization of Notes and Domino databases, applications and related web pages that is consistent with the consolidation of information technology services in GSA and not only meets but exceeds the intention of Recommendation 3. The planned actions will be completed by June 30, 2009.

Actions Taken and Underway:

1. Information Technology Council approval to redefine the Notes Infrastructure domains as a single domain for the physical structure and three responsibility areas – FAS, PBS, and All Other (OCIO). FAS and PBS assume responsibilities for their specialized applications. OCIO assumes responsibility for the Notes infrastructure, for OCIO and GM&A specialized applications, and for agency-wide general databases. ITC approval June 17, 2008

2. Certify and Accredit Notes Infrastructure with the Authorizing Officials being the FAS, PBS, and GSA CIOs. Notes boundaries for OCIO responsibility include the Notes GEMS/GNNI back-end infrastructure, including the COOP site in Ft. Worth. Completed March 2009.

3. Identification of Notes servers by regional management and administrator with high level identification of types of applications and databases. Completed March 2008.

4. Plain language identification of the existing Notes and Domino databases and applications, by server and by Service ownership, in each region. Completed July 2, 2008.

5. ITC approval of Notes and Domino databases and applications ownership responsibilities, transition processes, and governance approach. ITC approval July 2, 2008

6. Give back to the Services their servers with remaining Notes databases on them. Services take custody of and responsibility for their Notes servers. Reported to ITC August 12, 2008. Transfers completed December 2008.

7. Implement governance procedures. Launched August 2008. Completion dates for individual actions vary.
   a. Charter the applications change control board. Completed as part of the new IT governance package. The new Enterprise Applications and Services Committee will function as the change control board.
   b. OCIO begin database scrubbing processes, deleting unused databases and identifying those that should be consolidated or redesigned. Began October 2008.
   c. FAS and PBS undertake their own database scrubbing processes, deleting unused databases and identifying those that should be consolidated or redesigned. Begun in September 2008.

IMPLEMENTATION REVIEW OF ALERT REPORT ON
SECURITY OF GSA'S ELECTRONIC MESSAGING SERVICES
AND NATIONAL NOTES INFRASTRUCTURE
REPORT NUMBER A070180/O/T/W07001
DATED SEPTEMBER 12, 2007
ASSIGNMENT NUMBER A100099

APPENDIX D - GSA-CIO'S RESPONSE TO THE DRAFT LETTER REPORT

GSA

GSA Office of the Chief Information Officer

March 31, 2010

MEMORANDUM FOR GWENDOLYN A. MCGOWAN
DEPUTY ASSISTANT INSPECTOR GENERAL FOR
INFORMATION TECHNOLOGY AUDITS (JA-T)

FROM: CASEY COLEMAN
CHIEF INFORMATION OFFICER (I)

SUBJECT: Implementation Review of Alert Report on Security of GSA's Electronic Messaging Services and National Infrastructure, Report Number A07010/O/T/W07001, dated September 12, 2007, Assignment Number A100099

This is in response to the IG draft Implementation Review of Alert Report on Security of GSA's Electronic Messaging Services and National Infrastructure.

My staff has reviewed the draft report and we concur with your findings and recommendations.

If you or your staff have any questions or require additional information, please contact Daryle Seckar, Director of Enterprise Management Services, on 202-208-5054.

U.S. General Services Administration
1800 F Street, NW
Washington DC 20405-0002
www.gsa.gov

IMPLEMENTATION REVIEW OF ALERT REPORT ON
SECURITY OF GSA'S ELECTRONIC MESSAGING SERVICES
AND NATIONAL NOTES INFRASTRUCTURE
REPORT NUMBER A070180/O/T/W07001
DATED SEPTEMBER 12, 2007
ASSIGNMENT NUMBER A100099

APPENDIX E – REPORT DISTRIBUTION

	Copies
Deputy Administrator, Office of the Administrator (A)	3
Chief Information Officer, Office of the Chief Information Officer (I)	3
Chief Financial Officer, Office of the Chief Financial Officer (B)	2
Commissioner, Federal Acquisition Service (Q)	1
Commissioner, Public Buildings Service (P)	1
Regional Administrator, New England Region (1A)	1
Regional Administrator, Northeast and Caribbean Region (2A)	1
Regional Administrator, Mid Atlantic Region (3A)	1
Regional Administrator, Southeast Sunbelt Region (4A)	1
Regional Administrator, Great Lakes Region (5A)	1
Regional Administrator, Heartland Region (6A)	1
Regional Administrator, Greater Southwest Region (7A)	1
Regional Administrator, Rocky Mountain Region (8A)	1
Regional Administrator, Pacific Rim Region (9A)	1
Regional Administrator, Northwest and Arctic Region (10A)	1
Regional Administrator, National Capital Region (11A)	1

	Copies
Assistant Inspector General for Auditing (JA)	2
Internal Control and Audit Division (BEI)	1
Deputy Assistant Inspector General for Real Property Audits (JA-R)	1
Deputy Assistant Inspector General for Finance and Administrative Audits (JA-F)	1
Deputy Assistant Inspector General for Acquisition Audits (JA-A)	1
Regional Inspector General for Auditing (JA-W)	1
Regional Inspector General for Auditing (JA-2)	1
Regional Inspector General for Auditing (JA-3)	1
Regional Inspector General for Auditing (JA-4)	1
Regional Inspector General for Auditing (JA-5)	1
Regional Inspector General for Auditing (JA-6)	1
Regional Inspector General for Auditing (JA-7)	1
Regional Inspector General for Auditing (JA-9)	1
Administration and Data Systems Staff (JAS)	1
Assistant Inspector General for Investigations (JI)	1