SOCIAL SECURITY

MEMORANDUM Refer To:

Date: September 10, 2004

To: Martin H. Gerry
Deputy Commissioner
for Disability and Income Security Programs

From: Assistant Inspector General
Audit

Subject: Evaluation of the Accelerated eDib System – Sixth Assessment (A-14-04-15005)

The Social Security Administration's (SSA) Office of the Inspector General has completed its sixth assessment in our ongoing evaluation of the Accelerated eDib (AeDib) initiative (formally the Electronic Disability or eDib initiative). We conducted this sixth assessment from April 2004 through August 2004 at SSA Headquarters in Baltimore, Maryland. While we did not conduct an audit of the AeDib initiative, our assessment addresses issues that further secure the processing of sensitive SSA information by the Disability Determination Services offices (DDS).

BACKGROUND

The enhancement of DDS systems to support paperless claims processing is included as one of the four major software initiatives for AeDib.[1] DDSs use a variety of hardware and software platforms to store, process, and protect sensitive SSA information. For example, as of March 2004, 51 IBM AS/400 midrange computers (AS/400) are used by 52 of the 54 DDSs[2] as the hardware platform for case processing. Sensitive SSA data,[3] processed and stored by each DDS, should be protected from inappropriate or unauthorized access, use, and disclosure.

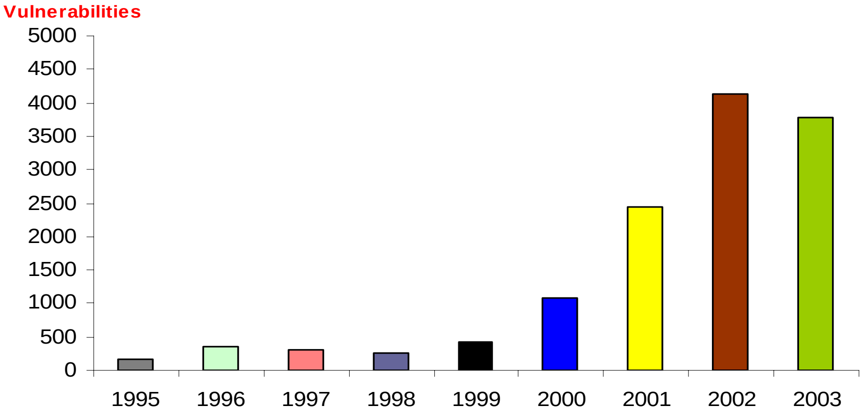
Operating system upgrade and maintenance procedures are one consideration in the overall security and administration of a DDS AS/400. Operating system upgrades occur

[1] Final Report prepared by Booz Allen Hamilton, *eDib Program Management Plan*, January 31, 2002, page II-4.
[2] The 52 DDSs include 48 States, District of Columbia, Puerto Rico, Guam and the Virgin Islands. Guam and the Virgin Islands disability cases are processed on an AS/400 located in the Western Program Service Center. Nebraska and New York use a different hardware platform.
[3] Sensitive data downloaded from SSA to the DDS claims processing system include claimant SSN, name, address, phone number, and date of birth.

when a DDS installs a new version/release of the AS/400 operating system.[4] Operating system maintenance is achieved by installing fixes provided by IBM.[5] DDSs that subscribe with IBM, receive alerts[6] of AS/400 fixes.

The Government Accountability Office[7] (GAO) reported[8] that patch management[9] is a critical process used to help alleviate many of the challenges involved with securing computing systems from attack. Figure 1 illustrates the dramatic growth in security vulnerabilities from 1995 to 2003.

Figure 1. Security Vulnerabilities 1995-2003



Source: GAO analysis based on Carnegie-Mellon University CERT® Coordination Center

GAO stated that from 1995 to 2003 the CERT® Coordination Center[10] reported just under 13,000 security vulnerabilities that resulted from software flaws.

The SSA and its affiliated DDSs each year request about 15 million medical and other records on behalf of claimants for Social Security disability benefits. SSA stated that the Document Management Architecture (DMA) project, which includes electronic medical evidence, is part of the AeDib effort that will create paperless automation to improve the disability claim processing. DMA is an Agency-level initiative to define and develop the architecture and an infrastructure to address the known and future document capture, indexing, storage, retrieval, and management needs. The electronic medical evidence project gives medical providers electronic options for submitting records and reports on behalf of disability claimants.

[4] IBM released Version 5 Release 3 of the operating system in June 2004. Version 5 Release 2 of the operating system is considered current for DDSs because the latest release has not been tested.
[5] IBM periodically creates fixes to correct problems or potential problems found within a particular IBM licensed program. Fixes can consist of documentation and/or code. Fixes are also called Programming Temporary Fixes (PTFs). A PTF is temporary only in the sense that it disappears because it is integrated in the next release of the operating system.
[6] Alerts provide automatic problem prevention notification and defect identification and resolution information specific for a DDS operating system.
[7] The Government Accountability Office was formally known as the General Accounting Office.
[8] GAO Report GAO-04-816T, Information Security: Agencies Face Challenges in Implementing Effective Software Patch Management Processes, June 2, 2004, pages 3 and 4.
[9] Patch management is the process of applying software code into a program to temporarily fix a defect.
[10] This a center of Internet security expertise at the Software Engineering Institute, a Federally funded research and development center operated by Carnegie-Mellon University.

In the paper environment, consultative examinations are submitted to the DDSs with a signature. This signature "… attests to the fact that the medical source doing the examination or testing is solely responsible for the report contents and for the conclusions, explanations, or comments provided with respect to the history, examination, and evaluation of laboratory test results."[11] To increase the medical providers' use of electronic records in lieu of paper records, SSA has developed a free, easy-to-use website called eData that can safely upload the electronic medical evidence.

As defined by the National Institute of Standards and Technology (NIST),[12] "Electronic authentication (e-Authentication) is the process of establishing confidence in user identities that are electronically presented to an information system." Each e-Government application should be rated by its Agency on a 1 to 4 scale where Level 1 provides the lowest authentication assurance and Level 4 provides the highest assurance. An agency determines the assurance level of its application by conducting an e-Authentication Risk Assessment. As the consequences of an authentication error becomes more serious, the required level of assurance increases and determines what controls should be in place. Including other controls that vary according to the assurance level, remote authentication is generally determined by the application's users presenting some secret only they know or possess, such as a password.

For Electronic Consultative Examination (eCE) submissions via eData, the authenticity of the submission is determined by the following process. First, the DDS invites a CE provider to participate in the process and if the invitation is accepted, the DDS and SSA coordinate to establish an authorized Internet account. Next, after the medical provider completes a valid logon onto SSA's Internet account, the CE provider links the electronic versions of the CE report and medical evidence to the submission screen and designates which DDS will receive the files. To submit these files, the CE provider must click the Internet "Agree" button on the Click and Sign Certification screen (see Attachment D). Clicking on the "Agree" button creates the CE provider's electronic signature that certifies the accuracy of the eCE files submitted. The process ends with the Agency sending the CE provider a confirmation message. This certification process is referred to by the Agency as eCE Click and Sign.

The purposes of our sixth assessment of AeDib were to: (1) determine whether the Agency has implemented an operating system upgrade and maintenance program for the IBM AS/400 computer systems used at DDSs; and (2) review the effectiveness of the Agency's authentication risk assessment in addressing the risks associated with the eCE Click and Sign process.

[11] *See* 20 C.F.R. §§ 404.1519n(e), 416.919n(e).

[12] NIST Special Publication 800-63, version 1.0, "*Electronic Authentication Guideline*", June 2004, page vi.

RESULTS OF OUR EVALUATION

We identified two areas of concern.

1. AS/400 operating system upgrade and preventive maintenance fixes were not current for DDS AS/400s. As a result, AS/400s are vulnerable to unnecessary system failures or breaches of security. Improvements are needed in the policies and procedures for the DDS AS/400 upgrade and maintenance guidance.

2. The eCE Click and Sign process for consultative examinations began as the DMA application risk assessment was concluding. As a result, there is a possibility that all risks for the Click and Sign process have not been identified. Now that the eCE Click and Sign process is expanding from a pilot, additional risks need to be considered.

Suggestions for an Operating System Version Upgrade and Maintenance Program

We analyzed the fourth quarter Calendar Year (CY) 2003 and first quarter CY 2004 IBM Performance and Information Reports.[13] As of March 2004, we determined that 31 of the 51 DDS AS/400 systems had noncurrent operating systems.[14] Only 1 of the remaining 20 systems with current operating systems and none of the 31 noncurrent operating systems had a 2004 cumulative fix level. A cumulative fix level is the primary method of performing preventive maintenance for AS/400 operating systems. It is usually issued quarterly and contains a cumulative package of group and individual fixes issued more frequently. We were advised that the information contained in this report is not validated by SSA for accuracy. In addition, except for observing the cumulative fix level in the report, SSA does not know whether DDSs are current with fix updates.[15] See Attachment A for a listing of State Operating System Data by region.

SSA has made great strides to upgrade the operating systems for the AS/400s used by DDSs. In December 2003, 46 of the 51 DDS AS/400 systems had noncurrent operating systems. However, 15 upgrades were accomplished from December to March, which reduced the number of noncurrent operating systems to 31 and we were advised that as of July 14, 2004, only four DDSs require upgrades. These strides were achieved to allow SSA to take advantage of the Websphere MQ Series functionality[16] in support of AeDib, not for version control purposes. Likewise, the cumulative fix levels for 21 AS/400s improved from December to March.[17] However, because such a large number of DDS systems have not installed a 2004 cumulative fix level, improvements in the program are needed to ensure systems are updated.

[13] This quarterly report was designed for SSA to monitor the performance metrics of the AS/400 systems at DDSs. It also includes operating system version and maintenance data.

[14] The current operating system used by DDSs is version 5 release 2.

[15] IBM issues a variety of fix updates. A description of those updates is presented in Attachment B, Program Temporary Fixes.

[16] Websphere MQ Series allows SSA to easily exchange information across different computer platforms, integrating existing business applications in the process.

[17] Thirteen of the improvements were attributable to the operating system upgrade.

SSA's draft national disaster recovery plan for DDS AS/400s[18] is less effective if the operating system version on the AS/400 maintained at the National Computer Center (NCC)[19] is not the same as those in the DDSs. The NCC AS/400 is using version 5 release 2 of the operating system, which is more current than 31 DDSs, as of March 2004. We were advised that cases processed on an AS/400 with an earlier version of the operating system will not function on a newer release of the operating system.

If a DDS remains on a noncurrent AS/400 operating system release too long, it is likely to incur higher costs for an upgrade. Higher costs are incurred when a DDS needs to do a multiple step upgrade, which would require implementing an interim release just to be able to upgrade to the latest release. Upgrade costs are further increased if subsequent releases, which supported a single step upgrade, are withdrawn from marketing. In most of these cases, a DDS would then need to hire custom services to perform a potentially labor intensive upgrade from the back-level release to a current one.

If DDSs are not current with maintenance fixes, they increase the risk of unplanned outages, system failures, and/or security breaches. A fix maintenance strategy is recommended by IBM to potentially reduce the impact on operations that result from unplanned outages and program failures. In July 2004, we identified 5 security fixes issued in 2004 for the 20 DDS AS/400s on a current operating system. Because SSA limits its tracking of fix updates to a review of the cumulative fix levels in the quarterly IBM Performance and Information Reports, it would not know whether all necessary fixes have been tested and installed by the DDSs. SSA needs a process to determine whether other necessary fixes, such as individual fixes made available to DDSs with IBM alerts have been tested and installed.

The DDSs are expected to provide a controlled environment that meets SSA's minimum security requirements. The *DDS Security Document* (*DSD*)[20] was established as a comprehensive approach to DDS security in August 2001. In January 2002, SSA issued a supplement for the *DSD*, which contains policies, procedures, and recommendations for providing security on the AS/400.[21] In September 2003, SSA issued an update to the *DSD*, merging the AS/400 supplement into the *DSD*. Unfortunately, as the supplement was merged into the updated version of the *DSD*, the AS/400 upgrade and maintenance guidance in the supplement was omitted.[22] See Attachment C for the AS/400 Operating System Upgrade and Maintenance Guidance contained in the supplement.

[18] Draft *National Disaster Recovery Plan for IBM AS/400 (i-Series) Processors in the Disability Determination Services*, July 2003.

[19] In the event of a disaster, the DDS cases would be processed on this AS/400 until arrangements can be made for a permanent replacement of the AS/400 at the DDS.

[20] *Disability Determination Services Security Document*, September 2003.

[21] *Disability Determination Services Security Document Supplement, AS/400 Platform Security Settings*, January 31, 2002.

[22] *Disability Determination Services Security Document Supplement, AS/400 Platform Security Settings*, Chapter IV, Upgrade and Maintenance Guidance, January 31, 2002, pages 19 to 23.

There are no documented SSA guidance and procedures to monitor and enforce the implementation of current operating system versions and fixes for all DDSs processing cases on an AS/400 and the NCC AS/400 used for the National DDS disaster recovery planning. For the most part, SSA relies on IBM for these programs. We encourage the Agency to:

- Restore the AS/400 operating system upgrade and maintenance guidance for DDSs that was contained in the January 2002 AS/400 supplement.

- Establish and implement policies and procedures to monitor and enforce AS/400 operating system upgrade and maintenance for all DDS AS/400s promoting greater involvement of SSA in the process.

- Extend the AS/400 security settings monitoring to include AS/400 operating system upgrades and maintenance fixes, if feasible.

Risk Related Suggestions for the eCE Click and Sign Process

We reviewed the Agency's E-Authentication Risk Assessment and its Risk Mitigation Strategy for the piloted eCE Click and Sign process. Although we believe SSA has taken significant steps for meeting its goal to provide reasonable assurance[23] that the sender of the eCE has been authenticated, a broader-scoped risk assessment is needed to address risks not covered by these documents. We based our conclusions on our interviews with project personnel, our review of the documentation provided, and our comparison of these documents to the risk assessment portion of the Office of Management and Budget's (OMB) e-Authentication Guidance.

We reviewed the Agency's authentication risk assessment and mitigation reports for the eCE Click and Sign process and determined that the Agency's risk assessment complied with the applicable sections[24] of the OMB criteria. The OMB criteria require the completion of the following five steps to determine the appropriate assurance level:

- Conduct a risk assessment of the e-Government system.
- Map Identified risks to the required assurance level.
- Select technology based on the NIST e-Authentication technical guidance.
- After implementation, validate that the information system has operationally achieved the required assurance level.

[23] GAO/AIMD-00-21-3.1, *Standards for Internal Control in the Federal Government*, November 1999, page 6 states, "No matter how well designed and operated, internal control … provides reasonable, not absolute, assurance of meeting agency objectives."

[24] Office of Management and Budget Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, December 16, 2003, Attachment A, Section 2, *Assurance Levels and Risk Assessments*, pages 4-14.

[27] OIG Memorandum, *Evaluation of the Accelerated eDib System - Fifth Assessment*, March 10, 2004.

- Periodically reassess the information system to determine technology refresh requirements.

The Agency's risk assessment included the first three of the five steps. Steps four and five of the criteria were not applicable because the process was still in the pilot phase when the Agency conducted its risk assessment.

After completing the e-Authentication risk assessment, the Agency developed a strategy to mitigate the risks identified. SSA's attentiveness to these areas should contribute to the effectiveness of the National implementation of the process.

We have three risk-related suggestions for the National implementation of the eCE Click and Sign process. First, as designed by OMB, the e-Authentication risk assessment is limited to the risks related to establishing the authenticity of the medical provider. It did not address other risks, which may have been included in the DMA application risk assessment, had the eCE Click and Sign process started sooner. Examples of risks not addressed by the e-Authentication risk analysis are:

- What controls are in place to ensure that the submitted eCE files are not modified or deleted/lost any time after their receipt by the DDS and used by other SSA components during the claim process?

- What controls are in place to prevent unauthorized physical and logical access to the eCE files?

We reviewed and commented on the DMA risk assessment in a prior memorandum.[27] In this memorandum, we reported that the DMA risk assessment needed updating. We encourage the Agency to include the eCE Click and Sign process when it updates its DMA risk assessment.

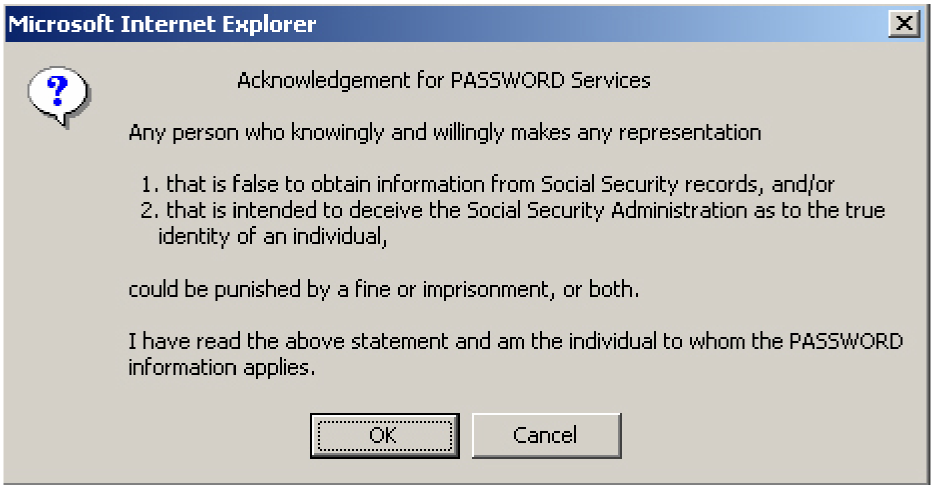
Second, the last SSA Internet screen accessed by a medical provider before submitting eCE contains language, which acts to certify that the medical provider is electronically signing for the eCE submitted. This screen, as seen on attachment D, has language allowing the medical provider to certify that the eCE is accurate. However, it does not provide the information that this certification is "under the penalty of perjury" and that the eCE is accurate. Although, we realize that paper consultative examinations do not contain the "under the penalty of perjury" clause, we encourage the Agency to consider adding this clause to the aforementioned screen. The addition of this clause may assist Federal, State, and local prosecutors, as well as SSA attorneys with any fraud prosecutions or other Social Security litigation involving this new process.

Third, the regulations[29] concerning the signature requirements are quite specific that the CE examination reports will be "… personally reviewed and signed by the medical source who actually performed the examination." Also, the regulations state that the use of a rubber stamp signature or the "… medical source's signature entered by any

[29] *See* 20 C.F.R. §§ 404.1519n(e), 416.919n(e).

other person is not acceptable." The electronic equivalent of signing the report by someone other than the medical provider is for someone to obtain and use the medical provider's username and password to submit eCE. To promote greater security and discourage medical provider's from sharing their username and password, we encourage the Agency to add a popup window similar to Image 1 below as the medical provider begins to login to the eData website. Image 1 shows the popup screen accessed before a user can obtain a password to access information about their benefits on SSA's online Social Security Password Services. The addition of this window may assist Federal, State, and local prosecutors, as well as SSA attorneys with any fraud prosecutions or other Social Security litigation involving this new process.

Image 1 Social Security Password Services Popup Window, Acknowledgement for Password Services.



Acknowledgement for PASSWORD Services

Any person who knowingly and willingly makes any representation

1. that is false to obtain information from Social Security records, and/or
2. that is intended to deceive the Social Security Administration as to the true identity of an individual,

could be punished by a fine or imprisonment, or both.

I have read the above statement and am the individual to whom the PASSWORD information applies.

OTHER MATTERS

SSA has initiated a process where claimants no longer have to physically sign a paper application when they file for Social Security and Supplemental Security Income benefits. On February 4, 2004, Commissioner Barnhart approved the adoption of the signature proxy alternatives. Click and Sign is one of those alternatives. Click and Sign is achieved when a claimant clicks an Internet 'sign' button representing an affirmation of the accuracy of the data and intent to file. In recognition of the significance of the Click and Sign process to the Agency, the Office of Inspector General is considering a review of the proxy-signature process used for benefit claims.

There is no expectation for the Agency to formally respond to this document. If you have any questions or comments, please call me or have your staff contact Kitt Winter, Director, Data Analysis and Technology Audit Division at (410) 965-9702, or Al Darago at (410) 965-9710.

Steven L. Schaeffer

Steven L. Schaeffer

Attachments

cc:
Thomas P. Hughes, Chief Information Officer for Social Security Administration
William E. Gray, Deputy Commissioner for Systems
Linda S. McMahon, Deputy Commissioner for Operations
Patrick P. O'Carroll, Jr., Acting Inspector General
Fritz Streckewald, Assistant Deputy Commissioner for Disability and Income Security Programs
Candace Skurnik, Director, Audit Management and Liaison Staff

State Operating System Data

SSA made significant improvements in the operating system versions and the cumulative fix levels between December 2003 and March 2004. Fifteen DDSs were upgraded from Version 5 Release 1 (V5R1) to Version 5 Release 2 (V5R2) of the operating system and 23 DDSs improved their cumulative fix levels. Wyoming improved its cumulative fix to a 2004 level.

The cumulative fix level is expressed as TL plus the Julian date of the cumulative release. For example, TL02050 is the 50th day of 2002 or February 19, 2002.

	Operating System Version/Release			Operating System Cumulative Fix Level		
State	12/31/03	3/31/04	Upgrade to v5r2 N-No	12/31/03	3/31/04	Improved N-No U-Unknown
Atlanta Region						
AL	V5R1	V5R2	1	TL03343	TL03252	N
FL	V5R2	V5R2	2	TL03252	TL03252	N
GA	V5R1	V5R1	N	TL03175	TL03175	N
KY	V5R1	V5R2	3	TL03175	TL03252	1
MS	V5R1	V5R2	4	TL03175	TL03252	2
NC	V5R1	V5R2	5	TL03343	TL03252	3
SC	V5R1	V5R2	6	TL03175	TL03252	4
TN	V5R1	V5R2	7	TL03175	TL03252	5
Boston Region						
CT	V5R1	V5R1	N	TL02134	TL03175	6
MA	V5R1	V5R2	8	TL03175	TL03252	7
ME	V5R1	V5R1	N	TL03175	TL03175	N
NH	V5R1	V5R2	9	TL03175	TL03252	8
RI	V5R1	V5R2	10	TL03175	TL03252	9
VT	V5R1	V5R1	N	TL03175	TL03175	N
Chicago Region						
IL	V5R1	V5R1	N	TL03175	TL03175	N
IN	V5R1	V5R2	11	TL03175	TL03252	10
MI	V5R1	V5R1	N	TL03175	TL03175	N
MN	V5R1	V5R2	12	TL03175	TL03252	11
OH	V5R2	V5R2	N	TL03252	TL03252	N
WI	V5R1	V5R1	N	TL03007	TL03175	12
Dallas Region						
AR	V5R1	V5R1	N	TL03175	TL03175	N
LA	V5R1	V5R1	N	TL03175	TL03175	N
NM	V5R1	V5R1	N	TL03175	TL03175	N
OK	V5R2	V5R2	N	TL03252	TL03252	N

	Operating System Version/Release			Operating System Cumulative Fix Level		
State	12/31/03	3/31/04	Upgrade to v5r2 N-No	12/31/03	3/31/04	Improved N-No U-Unknown
TX	V5R1	V5R2	N	TL03175	TL03252	13
Denver Region						
CO	V5R1	V5R1	N	TL03007	TL03175	14
MT	V5R1	V5R1	N	TL03175	TL03175	N
ND	V5R1	V5R1	N	TL03175	TL03175	N
SD	V5R1	V5R1	N	TL03175	TL03175	N
UT	V5R1	V5R1	N	TL03175	TL03175	N
WY	V5R1	V5R2	13	TL03175	TL04077	15
Kansas City Region						
IA	V5R1	V5R2	14	TL03175	TL03252	16
KS	V5R1	V5R1	N	TL03175	TL03175	N
MO	V4R5	V4R5	N		TL02169	U
New York Region						
NJ	V5R1	V5R1	N		TL03175	U
PR	V5R1	V5R1	N		TL03175	U
Philadelphia Region						
DC	V5R1	V5R1	N		TL03175	U
DE	V5R2	V5R2	N	TL03161	TL03252	17
MD	V5R1	V5R1	N	TL03007	TL03175	18
PA	V5R1	V5R1	N	TL03007	TL03175	19
VA	V5R1	V5R1	N	TL03175	TL03175	N
WV	V5R1	V5R2	15	TL03007	TL03252	20
San Francisco Region						
AZ	V5R1	V5R1	N	TL02134	TL03175	21
CA	V5R2	V5R2	N			U
CA-WPSC	V4R5	V4R5	N	TL02169	TL02169	N
HI	V5R1	V5R1	N	TL03175	TL03175	N
NV	V5R1	V5R1	N		TL03175	U
Seattle Region						
AK	V4R5	V4R5	N	TL02169	TL02169	N
ID	V5R1	V5R1	N	TL03175	TL03175	N
OR	V5R1	V5R1	N	TL03175	TL03175	N
WA	V5R1	V5R1	N	TL03175	TL03175	N

Programming Temporary Fixes

There are a variety of fixes to correct problems or potential problems found within a particular IBM operating system. Fixes can consist of documentation and/or code. Fixes are also called Programming Temporary Fixes (PTFs). DDSs need to assess whether a PTF is good for their operations. While cumulative PTFs are considered the primary method of preventive maintenance, they are not the only solution to an effective preventive maintenance strategy. Installation of high impact/pervasive (HIPER), group, and individual PTFs are also needed.

Cumulative PTF

A cumulative PTF package is the primary method of performing preventive maintenance for AS/400 operating systems. Cumulative PTFs are updated periodically (usually quarterly), and contain fixes for a specific release of the operating system and associated licensed programs.

A cumulative PTF package includes the following fixes.

- All HIPER group fixes for the release.
- The latest database group PTF for the release (for Version 5 releases only).
- All PTFs, including single PTFs and those in group PTFs, that have been ordered a minimum number of times when the package is created (normally 35 orders worldwide).

Group PTF

A group PTF is a single PTF number that includes multiple and individual PTFs for a specific function, such as database and HIPER PTFs. It allows a group of PTFs to be managed as a single entity to reduce complexity when dealing with PTFs.

HIPER PTF

HIPER PTFs fix serious or widespread problems. To prevent downtime on your server, IBM recommends that you install HIPER PTFs as soon as possible.

Individual PTFs

Individual PTFs are single PTFs. Individual PTFs that are not included in a group PTF or cumulative PTF package may be critical to DDS operations.

AS/400 Operating System Upgrade and Maintenance Guidance

IV. UPGRADE AND MAINTENANCE GUIDANCE

AS/400 Upgrades

SSA's AS/400 Operating System Upgrades

SSA has determined that a prudent software upgrade philosophy is to maintain a reasonably current, IBM-supported operating system product level while also assuring that DDS production systems continue to function normally. Our experience suggests that some version upgrades are more significant than others in terms of affecting functionality. When large changes are implemented in the operating system, it is more prudent to delay the upgrade until the version has been tested with the DDS application software.

DDSs should normally order an OS/400 release after one month, but no later than two months, after the release date of the *first cumulative Program Temporary Fixes (PTF) package* for the new release. The High Impact/Pervasive (HIPER) fixes should also be ordered at this time. It is also critical that all PTF cover letters be reviewed to identify any part of the cumulative PTF package that should not be applied.

For a system upgrade, the vendor of the DDS case processing system should first order and evaluate the upgrade timely. Once the vendor has completed testing/research and can be assured that DDS applications will function normally on the new operating system level, or that any necessary program changes have been made, the vendor and DDS should coordinate the OS/400 software upgrade on the DDS' AS/400s. If the vendor is an IBM Business Partner, they should receive advance copies of new versions or releases of the Operating System shortly after the GA announcement. This will allow them to make sure that their applications are fully compatible with the new release.

The OS/400 software upgrade should normally be installed on the first AS/400 in a DDS within one month after physically receiving the software upgrade. *However, if DDSs obtain upgrade support from a vendor, the installation schedule should be coordinated with the vendor.* At least 1 week should elapse between additional installations to guarantee stability for the other AS/400s.

Adherence to this software upgrade policy will enable any problems introduced with the OS/400 software to be experienced, identified, and resolved before the OS/400 software upgrade is propagated to additional AS/400 systems. In addition, following this software upgrade policy will enable the DDS AS/400s to maintain a reasonably current OS/400 operating system level.

To obtain new OS/400 releases/versions, DDS IT Staff should call their IBM National Customer Relationship Representative or IBM National Client Representative. They can also be obtained through the IBM DDS Gold Service contact in Atlanta, at (770) 863-1788.

IBM AS/400 Operating System Upgrades

OS/400 upgrades occur when IBM has developed a new version/release of the OS/400 Operating System and IBM Program Products. IBM does extensive testing of the new version or release of the Operating System prior to a General Availability (GA) announcement, i.e., a release to the general public. Generally, most IBM Business Partners (BPs), Value Added Retailers (VARs), and Application Developers (ADs), through their established relationship with IBM, get advanced releases or receive the new version or release of the Operating System shortly after the GA announcement. This allows them to make sure that their products are fully compatible with the new release.

There are several reasons for users to periodically upgrade their OS/400 Operating Systems. Every release of OS/400 has a defined Program Services period. The Program Services period begins when an OS/400 upgrade is announced/released. The ending date of the Program Services period is included as part of the announcement letter for that particular release of OS/400. During the Program Services period, IBM will accept reported problems with the release and, if necessary, IBM will produce corrective fixes. At the end of that Program Services period, IBM will no longer accept any problems for analysis.

Another reason to upgrade to a current release is that, once a release has reached its end of Program Services, a user will generally not be able to upgrade in a single step directly to a later release. If a user cannot upgrade directly to a new release, the user will need to do a multiple-step upgrade. In other words, the user will need to upgrade to an interim release, and then the user will need to upgrade to the latest release. A user can also remain too long on a release, so that if a number of subsequent releases have been made there may be no supported way for the user to upgrade the OS/400 Operating System. This situation may require expensive custom services to perform the upgrade from the user's back-level release.

AS/400 Maintenance

SSA's AS/400 Maintenance Policy

IBM releases Cumulative PTFs for the AS/400 Operating System and related products approximately every 3 months. IBM recommends that *"Cumulative PTF packages should be installed every three to four months if there is no change to the equipment or programs on your system"*.

SSA has determined that a prudent maintenance policy is to order the Cumulative PTF Package after 1 month of its release, but no later than 2 months after the release date. The HIPER PTFs for the Cumulative PTF maintenance should also be ordered when the Cumulative PTF Package is ordered.

The Cumulative PTF Package should normally be installed on the first AS/400 within 3 weeks after physically receiving the maintenance package. However, if a DDS obtains maintenance support from a vendor, the installation schedule should be coordinated with the vendor. At least 1 week should elapse between additional installations.

Adherence to this maintenance policy will enable any problems introduced with the Cumulative PTF Package to be experienced, identified, and resolved before the Cumulative PTF maintenance is propagated to additional AS/400 systems. In addition, following this maintenance policy will enable the DDS' AS/400s to maintain a reasonably current PTF maintenance level.

To obtain OS/400 Operating System maintenance products, DDS IT Staff can call the IBM AS/400 Support Line at (800) 237-5511, as well as order them through their IBM AS/400 Electronic Customer Support (ECS) (modem connection) and IBM's Technical Support Web site at http://www-912.ibm.com.

IBM AS/400 Operating System Maintenance

The second process in supporting the IBM AS/400 Operating System is regular maintenance. Maintenance includes the following alerts, fixes, and support:

Alerts
Alerts provide automatic problem prevention notification, defect identification and resolution information specific to your operating environment. SSA provides this service for all AS/400s that it has procured.

Program Temporary Fixes (PTFs)
PTFs are fixes for the OS/400 Operating System. They are code changes created to correct problems or potential problems found within either a particular IBM licensed program or a particular non-IBM program. PTFs are designed to replace one or more objects in the licensed program. Generally, PTFs are incorporated in a future full-release version of the operating system.

High Impact/Pervasive (HIPER) PTFs
HIPER PTFs are those that affect a majority of customers.

Cumulative PTF Packages (CUMs)
CUMs is the primary method of performing preventive maintenance on the OS/400 Operating System and IBM licensed programs. There are several reasons to routinely install CUMs. Cumulative PTF Packages contain recommended PTFs that will correct problems, or potential problems, with the OS/400 Operating System and IBM licensed programs; and they are updated on a periodic basis. A routine Cumulative PTF Package maintenance strategy will reduce the potential of unplanned outages and program failures.

Group PTFs
A Group PTF is a single PTF that provides a logical set of fixes affecting a specific function, e.g., database, HIPERs, etc. Group PTFs are dynamically updated when new fixes become available for the affected function.

Authorized Program Analysis Report (APAR)
APAR is a problem report specific to an IBM program (and release), with an associated fix (usually a PTF or workaround).

Standard Defect Support
The OS/400 Operating System comes with Standard Defect Support. If a customer suspects a code problem, they can call IBM if they have AS/400 Support Line; if they don't have AS/400 Support Line, they must email, fax, or mail their request to IBM. However, SSA provides ongoing IBM Support Line services for all AS/400s that have been purchased for the DDS and SSA communities. IBM will work with the customer to resolve the issue. If necessary, IBM will provide a work-around (APAR) or code fix (PTF). Standard support will always be for the current release plus one level back. When a new release/version is made available, three releases may be supported for a short period of time--the current new release plus the 2 previous levels.

Extended Usage Support
Extended Usage Support provides the standard AS/400 Support Line for versions/releases of OS/400 and associated IBM software products that are no longer current; i.e., the product is no longer sold and defect support has been discontinued. Generally, support is provided only for the current OS/400 release and the two previous releases.

Extended Defect Support
Extended Defect Support provides defect support (APARs and PTFs) for OS/400 and associated IBM software products that are no longer current; i.e., the product is no longer sold and standard defect support has been discontinued. Extended Defect Support is only available for a limited time. Without Extended Defect Support the "fix" would be to upgrade to the current release. It is unlikely that a PTF will be required for a release that is "out of support." Extended Defect Support is a temporary solution generally used by large customers with many machines who foresee the inability to bring their systems to a supported release in a timely fashion.

IBM AS/400 Software and Hardware Support Web Sites

Following are IBM Web Sites that provide detailed information on IBM AS/400 Operating System and Hardware support:

1. General Information on Program Services
   http://www-912.ibm.com/supporthome.nsf/document/10000080

2. Software Subscription
   http://www-1.ibm.com/servers/eserver/iseries/sftsol/subscript.htm

3. Support Line
   http://www-1.ibm.com/services/its/us/mus62d1.html

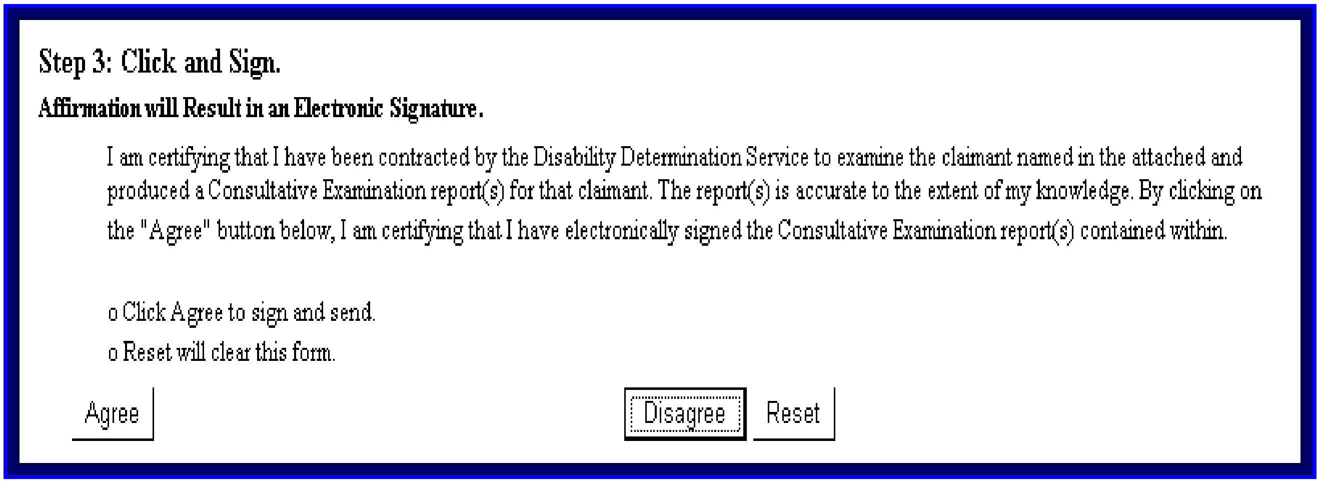
4. Alerts
   http://www-1.ibm.com/services/its/us/alert.html

5. Hardware Maintenance
   http://www-1.ibm.com/services/its/us/hardmain.html

Click and Sign Certification Screen

Once the medical provider has logged onto the Internet successfully and has identified which DDS is to receive the files containing the consultative examination (CE) files, a certification screen is displayed. By clicking on the “Agree” button, this screen creates the CE provider’s electronic signature that certifies the accuracy of the CE files submitted. The Agency refers to this process as the eCE Click and Sign. Image A shows the details of the eCE Click and Sign screen.

Image A Click and Sign Certification for Electronic Consultative Examination Submission



Step 3: Click and Sign.

Affirmation will Result in an Electronic Signature.

I am certifying that I have been contracted by the Disability Determination Service to examine the claimant named in the attached and produced a Consultative Examination report(s) for that claimant. The report(s) is accurate to the extent of my knowledge. By clicking on the "Agree" button below, I am certifying that I have electronically signed the Consultative Examination report(s) contained within.

o Click Agree to sign and send.

o Reset will clear this form.